CyberHubs

Informe de Análisis de Necesidades en Competencias de Ciberseguridad. España.

Co-funded by
the European Union

Sobre CyberHubs

La Red de Centros Europeos de Competencias en Ciberseguridad (CyberHubs) es un proyecto de tres años que nace con el objetivo de mejorar el ecosistema de capacidades en materia de ciberseguridad en Europa. El proyecto establecerá una red de siete centros de competencias en ciberseguridad en Bélgica, Estonia, Grecia, Hungría, Lituania, Eslovenia y España, que promoverá el desarrollo de capacidades digitales en esta área y apoyará el desarrollo de una mano de obra cualificada en este campo.

Los resultados esperados del proyecto incluyen el establecimiento de una red europea sostenible de centros de competencias de ciberseguridad (*Hubs*), el desarrollo de estrategias nacionales de competencias en ciberseguridad, la creación de soluciones innovadoras en el área a través de un Hackathon Europeo, el establecimiento de asociaciones a largo plazo y la colaboración con el ecosistema de ciberseguridad en general.

Socios del proyecto

CyberHubs reúne a 21 socios de pleno derecho de 11 Estados miembros europeos y 3 miembros asociados.

Socios de pleno derecho

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

Miembros asociados

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

Aviso legal

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados en este documento solo comprometen a sus autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de ellos.

Co-funded by the European Union

Análisis de Necesidades en Competencias de Ciberseguridad. España, 2024.

Entregable D2.1: «Análisis de desajustes de las competencias en ciberseguridad».

Autores: Alejandro Velásquez (Universidad Internacional de La Rioja - UNIR), Gaëlle Candel (AMETIC), Shila Ganguly (Universidad Internacional de La Rioja - UNIR).

Revisores: Daniel Burgos (Universidad Internacional de La Rioja - UNIR), Eduardo Valencia (AMETIC).

Historial de revisiones			
Versión	**Fecha**	**Modificado por**	**Versión**
0.1	4/07/2024	Shila Ganguly (UNIR)	Borrador (estructura)
0.2	15/07/2024	Gaëlle Candel (AMETIC)	Desarrollo capítulo 2
0.3	17/07/2024	Alejandro Velásquez (UNIR)	Desarrollo capítulos 4 y 5
0.4	29/07/2024	Shila Ganguly (UNIR)	Revisión y comentarios
0.5	20/08/2024	Gaëlle Candel (AMETIC)	Desarrollo capítulos 3 y 6
0.6	4/09/2024	Alejandro Velásquez (UNIR)	Integración de informes AMETIC. Revisión
0.7	16/09/2024	Gaëlle Candel (AMETIC)	Redacción de la introducción y comentarios
0.8	19/09/2024	Shila Ganguly (UNIR)	Edición. Revisión general
0.9	01/10/2024	Marie Montaldo (DIGITALEUROPE)	Revisión del documento
1.0	05/10/2024	Alejandro Velásquez (UNIR)	Integración sugerencias Digital Europe

Tabla de contenidos

Listado de Tablas

Listado de Gráficos

Resumen ejecutivo

Introducción

El Análisis de Necesidades de Ciberseguridad consiste en el estudio del estado actual de la ciberseguridad en España. Este informe contiene la información necesaria sobre todos los parámetros de interés para el hub español, que es uno de los objetivos clave del proyecto. Durante el análisis, se han recopilado datos sobre programas de ciberseguridad en diferentes universidades, así como documentos y referencias que posee el país para la planificación estratégica en ciberseguridad, regulaciones y políticas en el área. Además, la opinión de expertos en ciberseguridad ha respaldado la información recabada de empresas privadas y públicas en España a través de un cuestionario. Toda esta información se ha correlacionado con informes activos del mercado laboral y bases de datos en España.

Objetivo

El informe Análisis de Necesidades busca encontrar las necesidades críticas de competencias y roles profesionales relacionados con la ciberseguridad en España, teniendo en cuenta el ecosistema de ciberseguridad del país y sus oportunidades y peculiaridades. El objetivo es identificar y establecer los roles de ENISA en ciberseguridad, para así fortalecerlos. Dichos roles se refieren a perfiles de trabajo y responsabilidades específicos en el ámbito de la ciberseguridad, tal como se definen en ENISA (Agencia de la Unión Europea para la Ciberseguridad), que son cruciales para mantener y mejorar la seguridad digital de Europa. Para ello, el hub se centrará en la mejora de los programas educativos que abordan las necesidades del mercado laboral y las capacidades tecnológicas a nivel nacional. También se elaborará una Estrategia de Competencias de Ciberseguridad específica en cada país, contando con la información sobre demanda actual y futura de competencias y roles en ciberseguridad y con la oferta actual de programas de formación en ciberseguridad.

Enfoque

Este análisis adopta un enfoque multimétodo mediante el cual la recopilación de datos primarios y secundarios constituyen los datos de entrada para el análisis. Este enfoque incluye: i) una investigación documental (de la demanda) para obtener información sobre funciones y capacidades de ciberseguridad potencialmente claves junto con un estudio de la bibliografía existente (documentos científicos, informes del mercado laboral y bases de datos del mercado laboral) y un análisis de las ofertas de empleo, ii) un cuestionario para recopilar datos de la industria y otros agentes clave sobre las necesidades actuales y futuras en cuanto a funciones y competencias profesionales de ciberseguridad, iii) una investigación documental para obtener una visión general de la oferta actual de formación en ciberseguridad, y iv) un panel de expertos para explorar posibles escenarios futuros y validar los resultados de la recopilación de datos cuantitativos. Este enfoque metodológico utiliza como base marcos europeos, como el Marco Europeo de Capacidades en Ciberseguridad (ECSF) y otros marcos relevantes para especificar las principales misiones, tareas y competencias de ciberseguridad necesarias en el contexto profesional, lo que lo convierte en una referencia de alto valor para la elaboración de perfiles de competencias y conocimientos que necesitan los profesionales de la ciberseguridad.

Resultados

El resultado del informe muestra las áreas que deben mejorar en el campo de la ciberseguridad en España, identificando los roles de ENISA que requieren ser fortalecidos en términos de programas educativos, formación, desarrollo de competencias y capacidades tecnológicas. Abordar estas brechas creará mayores oportunidades

en el mercado laboral para roles que tienen una gran demanda, lo que ayudará a satisfacer la creciente necesidad de profesionales de ciberseguridad. Los resultados se resumen como sigue:
En primer lugar, dentro de los informes y diferentes estudios analizados y presentados en este informe, los roles más requeridos para este mercado laboral en crecimiento son los siguientes:

1. Implementador de Ciberseguridad (*Cybersecurity Implementer*).
2. Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*).
3. Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).
4. Responsable de Ciberseguridad en Jurídico, Legal y Cumplimiento (*Cyber Legal, Policy and Compliance*).
5. Responsable de Riesgos de Ciberseguridad (*Cybersecurity Risk Manager*).

En segundo lugar, y teniendo en cuenta el cuestionario, los roles en los que se espera una mayor demanda y crecimiento son los siguientes:

- Implementadores/Expertos en Ciberseguridad (*Cybersecurity Implementer/Expert*).
- Responsable de Seguridad de la Información (*Chief Information Security Officer*-CISO)/Gerente (sector público).
- Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).

Se evidencia que España requiere más profesionales en los siguientes roles por orden de importancia:

1. Implementador de Ciberseguridad *(Cybersecurity Implementer*).
2. Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*).
3. Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).

Conclusiones

Los roles más importantes y demandados en el sector son los Implementadores de Ciberseguridad (*Cybersecurity Implementer*), los Arquitectos de Ciberseguridad (*Cybersecurity Arquitect*) y los Expertos en Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*), que desempeñan un papel crucial en la gestión de la seguridad digital de las organizaciones.

Los roles y necesidades de los profesionales se centran en lenguajes de programación para la implementación, arquitectura y análisis de sistemas de ciberseguridad. La creciente demanda de expertos en ciberseguridad con habilidades técnicas y la alta valoración de habilidades críticas reflejan la importancia de estar preparados ante las amenazas cibernéticas, que están en constante evolución, y las tecnologías modernas.

Además, existe una brecha significativa entre la oferta y la demanda de profesionales de ciberseguridad en España, y el mercado laboral requiere más expertos con habilidades técnicas avanzadas. Esta brecha se ve exacerbada por la "fuga de cerebros", ya que muchos profesionales cualificados buscan nuevas oportunidades en el extranjero.

1 Introducción

1.1 Competencias de ciberseguridad en España

España se ha consolidado como un actor destacado en el panorama europeo de la ciberseguridad. La Estrategia Nacional de Ciberseguridad del país, que se actualiza continuamente, refleja un enfoque proactivo de la seguridad digital. A pesar de estos esfuerzos, siguen existiendo desafíos significativos, en particular la escasez de profesionales altamente cualificados necesarios para desempeñar funciones críticas, como implementadores de ciberseguridad, arquitectos y personal de respuesta a incidentes. La creciente adopción de tecnologías en la nube e inteligencia artificial, combinada con amenazas cibernéticas cada vez más sofisticadas, destaca la necesidad de capacitación especializada en áreas como programación y arquitectura de sistemas. Además, España se enfrenta a la competencia de otros países por el talento, lo que lleva a una "fuga de cerebros" de expertos en ciberseguridad. El sector público lucha por mantenerse al día ante la demanda de ciberseguridad, creando vulnerabilidades en la protección de la infraestructura nacional.

1.2 Enfoque de la investigación

La metodología para analizar las necesidades de competencias de ciberseguridad específicas de cada país es común en los siete países que representan a CyberHubs: Bélgica, Estonia, Grecia, Hungría, Lituania, Eslovenia y España. Se ha utilizado el Marco Europeo de Capacidades en Ciberseguridad (ECSF) como punto de partida para definir las capacidades y los conocimientos necesarios en las funciones profesionales de ciberseguridad. La metodología se basa en un enfoque multimétodo para recopilar y analizar datos cuantitativos y cualitativos de múltiples fuentes, con el objetivo de identificar los requisitos actuales y emergentes de competencias de ciberseguridad, así como los roles profesionales. La recopilación y el análisis de datos se han centrado tanto en la demanda como en la oferta de competencias y roles de ciberseguridad en España.

El primer paso ha consistido en identificar la demanda actual y futura de roles, competencias, habilidades y conocimientos de ciberseguridad mediante una investigación documental, un cuestionario, un panel de expertos y un análisis de ofertas de empleo. La segunda parte del análisis se ha centrado en identificar programas de formación existentes, con el objetivo de determinar en qué medida la oferta actual de formación en ciberseguridad es suficiente para satisfacer la demanda. Por último, se ha realizado un análisis de deficiencias, comparando la demanda actual y futura con la oferta existente.

Gráfico 1: Recopilación y análisis de datos sobre la demanda y la oferta

El análisis de necesidades proporciona una información valiosa para el desarrollo de estrategias nacionales en la mejora de competencias en materia de ciberseguridad. El análisis de deficiencias juega un papel fundamental en la evaluación general de necesidades, ayudando a alinear la demanda futura de roles y habilidades de ciberseguridad con la oferta futura de programas de formación, para así desarrollar estrategias de ciberseguridad más efectivas en cada país.

1.3 Guía de lectura

Este documento se ha estructurado para proporcionar primero una instantánea del entorno de ciberseguridad de España, seguido de un análisis detallado de las competencias necesarias para satisfacer la creciente demanda de profesionales en ciberseguridad. Concluye con recomendaciones para abordar el actual desajuste de competencias, centrándose en la educación, los programas de formación y la colaboración entre el Gobierno, el mundo académico y la industria para reforzar el ecosistema de ciberseguridad de España.

2 Investigación documental (demanda)

2.1 Recopilación de datos

Se ha llevado a cabo un proceso integral de recopilación de datos para obtener información en el campo de la ciberseguridad, con un enfoque específico en España. Así, la investigación abarca una amplia gama de fuentes, que incluye literatura académica e informes del mercado laboral, para proporcionar una comprensión holística de la temática.

A continuación, se muestra un desglose del número de elementos incluidos en el análisis:

Revisión bibliográfica:

1. Gobierno de España, "España Digital 2026":
    - Enlace: https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx.
2. Estrategia Nacional de Ciberseguridad, "Una prioridad, un reto y un compromiso para todos". Estrategia Nacional de Ciberseguridad, Gobierno de España, 2019. Incluye:
    - Amenazas y desafíos en el ciberespacio.
    - Finalidad, principios y objetivos de la ciberseguridad.
    - Resumen ejecutivo de la Estrategia Nacional de Ciberseguridad 2019.
    - Enlace 1: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.
    - Enlace 2: https://www.aesseguridad.es/news/55/Noticia_03_Estrategia_Nacional_Ciberseguridad.pdf.
3. CCN-CERT, «Approach to Artificial Intelligence and Cybersecurity» (Enfoque de la inteligencia artificial y la ciberseguridad). Informe sobre buenas prácticas, octubre de 2023. Incluye:
    - Tendencias emergentes.
    - Formación continua.
    - Enlace: https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/7190-ccn-cert-bp-30-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad/file.html.
4. UNE, «La normalización ayuda a prevenir los ciberataques y proteger las comunicaciones, trabajando en aspectos que tratan desde la seguridad en la nube hasta la gestión de pruebas electrónicas, desde la privacidad de IoT (Internet de las cosas) hasta la seguridad y privacidad de Big Data, entre otros». Artículo de la Asociación Española de Normalización, Grupo CTN320 sobre ciberseguridad.
    - Enlace: https://pasosfirmes.es/estandares-seguridad-informatica-ciberataques/.
5. Foro Nacional de Ciberseguridad, "Foro Nacional de Ciberseguridad. Motor de la Colaboración Público-Privada - 2023". El Foro Nacional de Ciberseguridad publicó un documento exhaustivo y de gran interés sobre el estado de la ciberseguridad en España, titulado "Foro Nacional de Ciberseguridad, motor de la colaboración público-privada - 2023", que incluye:
    - Marco de competencias para programas de formación superior especializada en ciberseguridad.
    - Informe sobre necesidades, capacidades y retos de la colaboración público-privada en ciberdefensa en las empresas de defensa.

- Enlace: FORO NACIONAL DE CIBERSEGURIDAD. MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA (foronacionalciberseguridad.es).

6. Deloitte, «El estado de la ciberseguridad en España - 2023». Incluye:
   - Análisis del estado de la ciberseguridad desde el punto de vista de los CISOs y responsables de ciberseguridad en España.
   - Enlace: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html.

7. Disruptive, «Cybersecurity Status Report 2023, Trends, Challenges and Opportunities in Cybersecurity» (Informe sobre el estado de la ciberseguridad 2023: tendencias, retos y oportunidades en materia de ciberseguridad). Incluye:
   - Tendencias.
   - Estrategias en España.
   - Enlace: https://ptedisruptive.es/wp-content/uploads/2023/12/Informe-situación-ciberseguridad-2023_compressed.pdf.

8. Revista Red Seguridad, "Cinco cosas que los profesionales de la ciberseguridad deben tener en cuenta en 2024". Artículo de la revista *Red Seguridad* sobre las competencias de los profesionales de la ciberseguridad y las tendencias futuras.
   - Enlace: https://www.redseguridad.com/.

Estudio del mercado laboral:

9. MordorIntelligence, "Mercado de Ciberseguridad en España Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)".
   - Enlace: https://www.mordorintelligence.com/industry-reports/spain-cybersecurity-market (en inglés).

10. Globaldata, España: «Tendencias laborales relacionadas con la ciberseguridad (octubre de 2023 - enero de 2024)».
    - Enlace: https://www.globaldata.com/data-insights/macroeconomic/spain-cybersecurity-related-job-trends-2094774/ (en inglés).

Bases de datos laborales:

11. Foro Nacional de Ciberseguridad, "Informe Sobre la Cultura de la Ciberseguridad en España". El Foro Nacional de Ciberseguridad publicó en 2021 un informe sobre la cultura de la ciberseguridad titulado «Informe sobre la cultura de la ciberseguridad en España», que incluye:
    - Alfabetización Digital en Ciberseguridad.
    - Propuesta de medidas que deben adoptarse en el ámbito de la educación.
    - Enlace: https://www.dsn.gob.es/sites/dsn/files/ACCESIBLE%20Trabajos_Foro-Nacional-Ciberseguridad.pdf.

12. INCIBE, "Análisis y Diagnóstico del Talento en Ciberseguridad en España - 2022". Estudio publicado recientemente, que incluye:
    - Diagnóstico del talento en ciberseguridad en España.
    - Definición de un modelo de caracterización de perfiles de ciberseguridad en España.
    - Enlace: https://files.incibe.es/incibe/talento/INCIBE_InformeCompleto_DIAG.pdf

13. Fundación Alternativas, «IV Informe sobre Ciencia y Tecnología en España – 2023, Tendencias, retos y oportunidades en ciberseguridad»:
    - Enlace: https://digital.csic.es/bitstream/10261/310469/3/Investigaci%c3%b3n_ciberseguridad_Espa%c3%b1a.pdf.

En total, se han analizado 13 elementos, que han proporcionado una visión global del panorama actual de la ciberseguridad en España, incluidas las tendencias, desafíos y oportunidades. Esta recopilación de datos constituye la base de la investigación y ha permitido extraer conclusiones significativas.

Tabla 1. Recopilación de datos en cifras

Recopilación de datos en cifras	
Literatura	8 artículos/documentos incluidos en el análisis
Investigación documental sobre el mercado laboral	2 informes sobre el mercado laboral
Base de datos laborales	3 informes de bases de datos laborales

España, en materia de ciberseguridad, es un referente en la Unión Europea. Su estrategia es una de las más completas y se actualiza constantemente a través de diferentes informes, que permiten mantener un enfoque real de la situación. Durante el desarrollo y recopilación de informes, documentos y análisis de ciberseguridad en España, se ha evidenciado la necesidad de más profesionales que cumplan con los perfiles en los que se centra este proyecto, para así aumentar la cobertura nacional de ciberseguridad y ciberdefensa.

El mercado laboral en España es amplio y abarca diferentes perfiles de ENISA. La investigación documental del mercado laboral ha permitido establecer una visión general de las tendencias y necesidades en ciberseguridad en las industrias privadas y públicas, así como en las instituciones que sirven al país.

En dichos informes y páginas web se puede observar, en términos generales, las principales necesidades del mercado laboral en España, pero principalmente se han identificado los perfiles más representativos que actualmente requieren un mayor interés por parte de los profesionales de la ciberseguridad.

2.2 Contexto nacional

España cuenta con una estrategia nacional de ciberseguridad, que enmarca, regula y lleva a cabo un análisis prospectivo a corto, medio y largo plazo de las acciones, actividades y necesidades de seguridad digital. En este análisis interviene el sector privado, público y gubernamental, todos alineados con la normativa interna e internacional para mantener, gestionar y satisfacer todas las necesidades, requisitos y acciones en materia de ciberseguridad.

2.2.1 Política y agencias

1. Acciones del Gobierno

   El gobierno español ha establecido el **Instituto Nacional de Ciberseguridad (INCIBE)** como la agencia encargada de coordinar las políticas y estrategias de ciberseguridad a nivel nacional. INCIBE colabora estrechamente con otras agencias gubernamentales, como el **Centro Nacional de Inteligencia (CNI),** el Ministerio de Economía y Transformación Digital y el **Centro Criptológico Nacional (CCN),** para promover la ciberseguridad en España. La **Guardia Civil y la Policía Nacional** cuentan con unidades especializadas en ciberdelincuencia.

   Además, el **Centro de Ciberseguridad Industrial (CCI)** se centra en la protección de los sistemas de control industrial y la ciberseguridad en el sector industrial.

2. Estrategia y directrices nacionales

   España cuenta con una Estrategia Nacional de Ciberseguridad que establece las líneas de actuación y objetivos para proteger al país frente a las ciberamenazas. Dicha estrategia engloba aspectos como la protección de infraestructuras críticas, la sensibilización pública y la promoción de la colaboración público-privada en materia de ciberseguridad. El documento es el siguiente: Estrategia Nacional de Ciberseguridad, 2019.

3. Campañas, iniciativas y oportunidades de financiación en España

   - Día de Internet Seguro: *Safe Internet Day* es una iniciativa anual para promover prácticas seguras online entre los ciudadanos españoles.
   - Programas de formación INCIBE: formación en ciberseguridad para profesionales y estudiantes.
   - Conferencias sobre seguridad de las TIC a cargo de la CCN.
   - Convocatoria de financiación de la Agenda Digital Europea: organizada en marzo de 2024, inversión de 84 millones de euros.
   - Iniciativa Estratégica para la Contratación Pública Innovadora (IECPI): herramienta promovida por INCIBE en 2021 para fomentar la innovación en ciberseguridad desde el sector público, concretamente mediante la adquisición de soluciones innovadoras o en fase de desarrollo.
   - Ciberseguridad de RETECH: iniciativa estratégica del país para el desarrollo del ecosistema de ciberseguridad (capacidades, industria, I+D, talento, etc.), que, con la coordinación de INCIBE, ha reunido en su primera fase 15 comunidades autónomas con un presupuesto inicial de 149 millones de euros.
   - Programa mundial de innovación en ciberseguridad: INCIBE, dentro del Programa Global de Innovación en Seguridad, tiene la misión particular de elevar las capacidades y recursos de ciberseguridad en los ecosistemas académico, empresarial y tecnológico, con el objetivo de impulsar las competencias de ciberseguridad de la sociedad y la economía en general.
   - Promoción externa de la industria a través de ICEX ESPAÑA (entidad pública empresarial nacional cuya misión es promover la internacionalización de las empresas españolas y la promoción de la inversión extranjera) y AMETIC.

2.2.2 Legislación y regulación

El panorama regulatorio en ciberseguridad en España abarca una combinación de legislación nacional y regulaciones de la Unión Europea (UE). Este marco tiene por objeto garantizar la protección de las infraestructuras críticas, los datos personales y los activos digitales contra las ciberamenazas.

En España existe un **Código de Ley de Ciberseguridad,** publicado en el Boletín Oficial del Estado, que cita las principales normas para tener en cuenta en relación con la protección del ciberespacio y la garantía de la ciberseguridad.

En este código, se hace referencia a las siguientes leyes, entre otras:

- **Esquema Nacional de Seguridad** (ENS) - Real Decreto 3/2010.
- **Ley de Seguridad Nacional:** Ley Orgánica 36/2015, de 28 de septiembre, de Seguridad Nacional, por la que se regulan los principios y organismos fundamentales, así como las funciones que deben desempeñar para la defensa de la Seguridad Nacional.

- **Orden TIN / 3016/2011,** de 28 de octubre, por la que se crea la Comisión de Seguridad en las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.
- **Ley 11/2002,** de 6 de mayo, por la que se regula el Centro Nacional de Inteligencia.
- Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la **Estrategia Nacional de Seguridad 2017.**
- **Estrategia Nacional de Ciberseguridad 2019**.

Las siguientes leyes abarcan también el área estudiada:

- Ley Orgánica de **Protección de Datos y Garantía de los Derechos Digitales** (LOPDGDD): Ley Orgánica 3/2018, de 5 de diciembre.
- Ley de **Servicios de la Sociedad de la Información y Comercio Electrónico** (LSSICE): Ley 34/2002, de 11 de julio.

La aplicación de la legislación de la UE, especialmente en el ámbito de la ciberseguridad, es supervisada por las autoridades españolas de acuerdo con los principios y directivas establecidos por la Unión Europea. España aplica las directivas y reglamentos de la UE a la legislación nacional, garantizando el cumplimiento de las normas y requisitos de la UE. Además, los reguladores españoles colaboran con agencias de la UE y participan en iniciativas y programas de la UE destinados a mejorar la ciberseguridad en los Estados miembros.

2.2.3 Mercado

El mercado de la ciberseguridad en España abarca una mezcla de grandes multinacionales, proveedores medianos y pequeñas empresas especializadas. Los jugadores clave incluyen:

- **Empresas multinacionales y grandes empresas:** Symantec Corporation, SIRT, Cisco Systems, Palo Alto Networks, IBM Security y Check Point Software Technologies son algunas de las empresas multinacionales que tienen una importante presencia en el mercado español, ofreciendo una amplia gama de soluciones de ciberseguridad para empresas y consumidores.

- **Proveedores medianos:** empresas como Panda Security, Fortinet, Trend Micro, Sophos, GMV y F-Secure Corporation ocupan un lugar destacado en el mercado español de ciberseguridad.

- **Pequeñas empresas especializadas:** por ejemplo, ElevenPaths (Telefónica), S21sec, CounterCraft, AlienVault (AT&T Cybersecurity), Vintegris, etc.

El valor global del mercado de la ciberseguridad en España, que incluye las ventas de software y hardware, así como los ingresos procedentes de la prestación de servicios, alcanzó los 1.950 millones de euros en 2022.

El mercado laboral es muy amplio y cambia continuamente, ya que depende de la evolución de las tecnologías de la información, y del crecimiento y descubrimiento de nuevas amenazas en el ciberespacio. Es evidente que hay una falta de profesionales en ciberseguridad a nivel internacional. España no se queda atrás en este aspecto, ya que al ser un referente, se requiere poder satisfacer las necesidades de la industria y las instituciones para proteger el entorno de la información y el ciberespacio. Esta es la razón por la que las personas que poseen un alto nivel de competencias tecnológicas son necesarias con cada vez mayor frecuencia. El problema radica en el tiempo y la dedicación que se requiere para adquirir estos conocimientos y habilidades, que son clave para el entorno de trabajo en ciberseguridad.

2.2.4 Sociedad

España es actualmente pionera en el establecimiento de estrategias y planes de innovación en tecnologías de la información, formación en todos los niveles académicos e implantación de nuevas tecnologías digitales de la información.

- **Digitalización:** según el informe DESI (Índice de la Economía y la Sociedad Digitales) de la Comisión Europea, España ha mostrado un progreso constante en su digitalización en los últimos años. Según el informe DESI 2022, España ocupó el séptimo lugar entre los 27 países de la UE en términos de digitalización. Este informe evalúa varios indicadores, como la conectividad, la digitalización de las empresas y las competencias digitales de la población.
- **Uso de herramientas digitales:** según el Instituto Nacional de Estadística (INE) de España, en 2023, el 95,4% de la población de entre 16 y 74 años ha utilizado Internet en los últimos tres meses (0,9 puntos porcentuales), el 55,9% ha comprado en Internet en los últimos tres meses (0,6 puntos más que en 2022) y el 66,2% tiene competencias digitales básicas o avanzadas. Estas cifras muestran una alta penetración de Internet y un uso generalizado de herramientas digitales entre la población española.
- **Sensibilización en materia de ciberseguridad:** el Instituto Nacional de Ciberseguridad (INCIBE) desarrolla iniciativas de sensibilización y formación en ciberseguridad dirigidas a ciudadanos, empresas y administraciones públicas.

España es un referente en ciberseguridad dentro de la Unión Europea, y muchos españoles desempeñan funciones de ciberseguridad en otros países de la región. Tal y como evidencia el informe de investigación documental de instituciones oficiales y no oficiales, y de programas de ciberseguridad, en el área de la educación existen excelentes oportunidades para profesionalizarse en temas relacionados con la ciberseguridad.

Empresas como Telefónica y Orange son un claro ejemplo de en el sector de las tecnologías de la información, manteniendo una competitividad y unos ingresos generados dentro del top 20 a nivel europeo, demostrando la necesidad de más y mejores profesionales en el ámbito de la tecnología y por tanto de la ciberseguridad.

2.2.5 Tecnología

Digital Spain 2026 es la actualización de la estrategia lanzada en julio de 2020 como hoja de ruta de transformación digital del país. Desde su presentación, se ha aprobado el Plan de Recuperación para España; se han publicado ocho planes específicos para su despliegue; se han puesto en marcha programas de inversión clave a nivel nacional, regional y local; y se han logrado avances decisivos en las reformas estructurales.

La actualización de la agenda de España Digital ha incorporado las prioridades para los próximos meses e incluido dos nuevos ejes transversales: Proyectos Estratégicos para la Recuperación y Transformación Económica (PERTE) y la iniciativa RETECH, una red de proyectos estratégicos emblemáticos de transformación en el ámbito digital propuestos por las comunidades autónomas.

El Gobierno español, a través del Instituto Nacional de Ciberseguridad (INCIBE), liderado por la Secretaría de Estado de Digitalización e Inteligencia Artificial, ha puesto en marcha la iniciativa RETECH Ciberseguridad. Este programa, respaldado por un presupuesto inicial de 149 millones de euros y la participación de 15 comunidades autónomas, tiene como objetivo fortalecer el ecosistema de ciberseguridad en España. Se espera que esta iniciativa impulse la investigación en tecnologías modernas, especialmente en el ámbito de la ciberseguridad, y fomente el desarrollo tecnológico en sectores estratégicos. Además, el Gobierno prevé invertir más de 530 millones de euros del Plan de Recuperación en proyectos de digitalización, lo que refleja una clara apuesta por el avance tecnológico en el país. La digitalización se está integrando en diversos sectores, desde el comercio electrónico hasta la administración pública y la industria, destacando el amplio alcance de los recursos digitales en la sociedad española.

2.3 Literatura

En este estudio se ha realizado una búsqueda de artículos y documentación relacionados con la formación, el talento y las tendencias futuras en el ámbito de la ciberseguridad:

- INCIBE, Análisis y Diagnóstico del Talento en Ciberseguridad en España, 2022.
- Deloitte, El estado de la ciberseguridad en España, 2023.
- Revista Red Seguridad, Cinco cosas a tener en cuenta por los profesionales de la ciberseguridad durante 2024.

2.3.1 Roles profesionales

Sobre la base de la información recopilada, se identificaron los roles profesionales más importantes en el campo de la ciberseguridad. Los más importantes incluyen:

- Responsable de Seguridad de la Información (*Chief Information Security Officer-CISO*): es uno de los roles más cruciales en una organización, en términos de ciberseguridad. El CISO es responsable de liderar la estrategia de seguridad de la información y garantizar que se implementen medidas efectivas para proteger los activos digitales de la empresa. Las conclusiones de este estudio reflejan una falta de este rol profesional en España.
- Arquitecto de Ciberseguridad (*Cybersecurity Architect*): dada la creciente adopción de servicios en la nube, los arquitectos de seguridad son fundamentales para diseñar e implementar soluciones de seguridad que protejan los datos y la infraestructura en dicho entorno.
- Analista de Seguridad de la Información (*Information security analyst*).
- Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).
- Ingeniero de Seguridad en Redes (*Network Security Engineers*).
- Implementador de Ciberseguridad (*Cybersecurity Implementer*).
- Hacker Ético (*Ethical Hacker*): su trabajo es crucial para probar la seguridad de una infraestructura y prevenir ataques maliciosos. Las conclusiones de este estudio reflejan una falta de hackers éticos en España.

En cuanto a previsiones futuras, se espera que los roles relacionados con la inteligencia artificial (IA) y la seguridad en la nube sean cada vez más importantes. Con la integración masiva de la IA en varias áreas de negocio y la creciente adopción de servicios en la nube, los profesionales de la ciberseguridad deberán entender todos los aspectos de seguridad relacionados con estas tecnologías. Además, se espera que los roles profesionales relacionados con la gestión de riesgos cibernéticos y la privacidad de los datos crezcan en importancia a medida que las empresas busquen cumplir con las regulaciones de protección de datos y enfrentar nuevas amenazas de seguridad.

2.3.2 Competencias

Las llamadas 'habilidades blandas' (*soft skills*) juegan un papel cada vez más importante en el éxito de los profesionales de la ciberseguridad. La capacidad de comunicarse de manera efectiva, tanto verbalmente como por escrito, es fundamental para colaborar con otros equipos y para comunicar los resultados y recomendaciones de seguridad a las partes interesadas no técnicas. Además, el pensamiento crítico y la

resolución de problemas complejos son esenciales para abordar unos desafíos que están en constante cambio y desarrollar soluciones innovadoras.

La capacidad de trabajar en equipo, la ética profesional y la integridad constituyen también competencias clave para los profesionales de la ciberseguridad, ya que a menudo trabajan en entornos colaborativos y deben tomar decisiones éticas sobre cómo proteger la información y los sistemas. La capacidad de adaptarse rápidamente a los nuevos entornos y tecnologías, así como de mantenerse al día sobre las últimas tendencias y amenazas en ciberseguridad, también son habilidades críticas para el éxito en este campo tan dinámico.

Las competencias técnicas (*hard skills*) son el baluarte de los profesionales de alto nivel en ciberseguridad. Estas competencias, desde los conocimientos más técnicos, permiten la implementación y configuración de sistemas y programas de ciberseguridad. Su comprensión y uso son esenciales para obtener resultados destacados en el campo de la ciberseguridad.

La programación de diferentes lenguajes, el conocimiento y configuración de redes, gestión de incidentes, análisis de malware y prueba de intrusión (*penetration tester*), son las herramientas técnicas de cualquier rol relacionado con ciberseguridad en empresas e instituciones privadas y públicas.

2.4 Informes y bases de datos sobre el mercado laboral

El trabajo se ha basado en los siguientes informes:

- MordorIntelligence, Análisis del tamaño y la cuota del mercado de la ciberseguridad en España - Tendencias y previsiones de crecimiento, 2024-2029 (*Cybersecurity Market in Spain Size & Share Analysis - Growth Trends & Forecasts, 2024-2029).*
- Globaldata, España: Tendencias laborales relacionadas con la ciberseguridad (octubre de 2023 - enero de 2024).
- INCIBE, Análisis y Diagnóstico del Talento en Ciberseguridad en España (2022).

El mercado de la ciberseguridad en España está experimentando un crecimiento significativo, con un valor estimado de 2.270 millones USD en 2024 y una previsión de 3.210 millones USD en 2029, lo que representa un crecimiento anual del 7,16%. Este aumento se debe a la digitalización en varios sectores, que ha expuesto a más entidades a ciberataques y ha dado lugar a una mayor demanda de servicios de seguridad. Sin embargo, a pesar de esta creciente demanda, queda patente la escasez de talento en el campo de la ciberseguridad, lo que plantea desafíos adicionales para satisfacer las necesidades del mercado.

La pandemia de COVID-19 agravó estos riesgos, con más de 150.000 ciberataques denunciados al Gobierno español desde su inicio. El aumento de la digitalización y del comercio electrónico están impulsando aún más la necesidad de soluciones en ciberseguridad para proteger los datos y la infraestructura crítica de las organizaciones.

En este contexto, el sector público está emergiendo como un motor clave del crecimiento del mercado, ya que la seguridad de la información y los datos sensibles son fundamentales para salvaguardar las operaciones y la integridad de las instituciones estatales. Se están implementando regulaciones más estrictas para fortalecer las medidas de seguridad cibernética en el país y garantizar la protección de infraestructuras críticas.

En cuanto a la industria de la ciberseguridad en España, está muy consolidada, con una gran competencia entre los principales actores. Se están estableciendo asociaciones estratégicas para fortalecer las capacidades

tecnológicas, ofrecer soluciones innovadoras a los clientes, mejorar la oferta de servicios de ciberseguridad y ampliar la cartera de productos disponibles en el mercado.

A pesar de la consolidación de la industria de la ciberseguridad en España, el informe de INCIBE de 2022 destaca un desafío importante: la escasez de talento cualificado. La creciente digitalización y el aumento de las ciberamenazas han generado una gran demanda de profesionales especializados, pero la formación actual no satisface las necesidades del sector. Aunque existen programas educativos, las competencias clave como las certificaciones CEH, OSCP o CISSP son insuficientes. Además, el informe destaca la baja representación de estudiantes de sexo femenino (solo el 18%) y la falta de docentes especializados.

2.4.1 Roles profesionales

Según el reporte 'Análisis y Diagnóstico del Talento en Ciberseguridad en España', en 2020 el país contaba con aproximadamente 149.774 profesionales en este campo, lo que representa el 0,26% del total de la población activa. Sin embargo, esta cifra es insuficiente para satisfacer las crecientes necesidades del sector. En 2020, se estimó que la demanda de profesionales de ciberseguridad alcanzaría los 63.191 puestos de trabajo. Este desajuste entre la oferta y la demanda se traduce en una escasez de 26.024 profesionales que España necesita incorporar para abordar los desafíos de seguridad digital.

Las proyecciones futuras sugieren que esta situación podría persistir e incluso intensificarse. El aumento exponencial de los ciberataques, como se mencionó anteriormente, (150.000 incidentes diarios de malware), junto con las nuevas regulaciones de ciberseguridad, está impulsando una demanda aún mayor. Por otro lado, más del 58% de las empresas españolas encuentran dificultades para encontrar personal cualificado en ciberseguridad.

Dentro de los informes y diferentes análisis consultados y presentados en este informe, los roles más requeridos para este creciente mercado laboral son los siguientes:

1. Implementador de Ciberseguridad (*Cybersecurity Implementer*).
2. Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*).
3. Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).
4. Responsable de Ciberseguridad en Jurídico, Legal y Cumplimiento (*Cyber Legal, Policy and Compliance*).
5. Responsable de Riesgos de Ciberseguridad (*Cybersecurity Risk Manager*).

2.4.2 Competencias

Como se puede observar en los roles profesionales más demandados en el mercado laboral español, se requiere un alto nivel de competencias técnicas (*hard skills*). Los tres perfiles más buscados por las empresas privadas son Implementador de Ciberseguridad (*Cybersecurity Implementer*), Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*) y el Experto en Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*). Estos tres roles requieren un alto nivel de conocimiento y preparación en ciberseguridad y sistemas tecnológicos, más concretamente en:

- Networking y Administración de Sistemas.
- Manejo y Respuesta de Incidentes de Seguridad.
- Comprensión de Sistemas Operativos.

- Control de Seguridad en Red.
- Prevención y Detección de Malware.
- Dominio en Codificación y Encriptación.
- Implementación y Gestión de Sistemas en la Nube.

2.5 Conclusiones

La principal barrera en el crecimiento del sector de la ciberseguridad en España es la escasez de talento cualificado. A corto plazo, se espera que este déficit continúe constituyendo un reto para el sector, impulsado por la creciente digitalización y el aumento de los ciberataques. Aunque las empresas se enfrentan a dificultades para cubrir los estos puestos, el establecimiento de asociaciones estratégicas y programas intensivos de formación podría aliviar parcialmente esta presión en los próximos años. Además, la implementación de nuevas regulaciones de ciberseguridad continuará impulsando la necesidad de profesionales especializados.

A largo plazo, la evolución tecnológica y los cambios regulatorios seguirán impulsando una creciente demanda de talento en ciberseguridad, lo que requerirá inversiones continuas en formación y desarrollo de competencias especializadas. Tanto el gobierno como las empresas deberán colaborar en el diseño de estrategias de educación y formación continua, así como en la creación de incentivos para atraer y retener talento cualificado en el área. Esto será crucial para abordar desafíos futuros en un entorno donde las amenazas cibernéticas son cada vez más sofisticadas.

Los roles más importantes y demandados en el sector son los Implementadores de Ciberseguridad (*Cybersecurity Implementers*), Arquitectos de Ciberseguridad (*Cybersecurity Arquitects*) y los Expertos en Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responders*), que desempeñan un papel crucial en la gestión de la seguridad digital de las organizaciones. También son esenciales los responsables de Riesgos de Ciberseguridad (*Cybersecurity Risk Managers*) y los responsables de Ciberseguridad en Jurídico, Legal y Cumplimiento (*Cyber Legal, Policy and Compliance*), roles que están ganando importancia debido al creciente número de regulaciones y políticas de ciberseguridad que las empresas deben cumplir.

3 Cuestionario

3.1 Recopilación de datos

El cuestionario se ha distribuido por correo electrónico a más de 100 organizaciones, cubriendo diversos sectores como Información y Comunicación; Actividades Profesionales, Científicas y Técnicas; y Administración Pública. También se publicó en la página de LinkedIn de AMETIC, que tiene más de 14.000 seguidores, y en la página de LinkedIn de UNIR iTED, con más de 600 seguidores, logrando una visibilidad significativa online. Además, se compartió en la cuenta X de AMETIC y en la cuenta UNIR iTED X para aumentar su alcance. El cuestionario ha sido respondido por muchas organizaciones, grandes y medianas empresas, reflejando la necesidad de implementar medidas firmes en ciberseguridad. Las respuestas cubren categorías como el sector o el tamaño de la organización, o la estructura de ciberseguridad establecida.

3.2 Resultados

En el contexto actual, la ciberseguridad se ha convertido en un área esencial en las organizaciones, independientemente de su tamaño o sector. La encuesta realizada por el CyberHub español proporciona una visión detallada de cómo las empresas estaban abordando esta creciente necesidad, centrándose en tres áreas clave: funciones, capacidades y formación en materia de ciberseguridad. Este análisis no solo revela las tendencias actuales, sino también las proyecciones futuras con respecto a los requerimientos y estrategias en el campo de la ciberseguridad.

3.2.1 Roles profesionales

Según las empresas encuestadas, los roles que se espera que vean la mayor demanda y crecimiento son los siguientes:

- **Implementador/Experto en Ciberseguridad** (*Cybersecurity Implementer/Expert*)**:** este es el perfil con mayor proyección de crecimiento. Actualmente, el 90,91% de las empresas ya cuenta con un implementador o experto en ciberseguridad, y se espera que la demanda de estos profesionales crezca un 38,56% en los próximos dos años. A largo plazo, esta demanda podría aumentar drásticamente en un 111,69%, lo que refleja la creciente necesidad de expertos que puedan implementar y administrar las soluciones de seguridad necesarias para proteger a las organizaciones contra las amenazas cibernéticas.
- **Responsable de Seguridad de la Información/Gerente (sector público)** (*Chief Information Security Officer-CISO*)**:** con un 77,27% de las empresas que ya cuentan con un CISO o gestor de seguridad de la información, este perfil también muestra un crecimiento en el futuro, aunque más moderado. Se prevé un aumento del 25% en la demanda de esta posición en los próximos dos años, y un aumento del 60% a largo plazo. Esto subraya la importancia de un liderazgo fuerte y estratégico en ciberseguridad que pueda dirigir y supervisar las políticas de seguridad de la organización.
- **Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*):** aunque el 63,64% de las empresas cuenta actualmente con este perfil, la demanda de estos profesionales es significativa, con un aumento proyectado del 56,25% en los próximos dos años. A largo plazo, se espera que la demanda de este perfil aumente en un 112.5%, destacando la necesidad crítica de estar preparados para responder de manera rápida y efectiva a cualquier incidente de seguridad.

El siguiente gráfico muestra el crecimiento esperado en la demanda de roles clave de ciberseguridad según las empresas encuestadas.

Gráfico1: Proyección del aumento de los roles de ciberseguridad

3.2.2 Competencias

En el ámbito de la ciberseguridad, es crucial no solo disponer de perfiles específicos dentro de las organizaciones, sino también de un conjunto de competencias técnicas y estratégicas que les permitan enfrentar amenazas cibernéticas. En las respuestas obtenidas en el cuestionario se han identificado las habilidades más valoradas y demandadas por las empresas. Éstas reflejan no solo la necesidad actual, sino también las áreas en las que las organizaciones están invirtiendo para asegurar su infraestructura y datos.

Como se muestra en la siguiente tabla, las competencias más demandadas incluyen:

- **Privacidad de Datos y Seguridad de Datos y Criptografía:** ambas competencias son de "gran necesidad", según el 56% de las organizaciones encuestadas. Esto subraya la importancia de proteger la información sensible y garantizar la seguridad de los datos a través de métodos criptográficos.
- **Seguridad en la Nube y Control de Acceso/Gestión de Identidades:** como en el punto anterior, el 48% de las organizaciones identifica que tiene una "gran necesidad" de estas habilidades. Con la creciente adopción de soluciones en la nube, estas competencias son esenciales para garantizar un acceso seguro y controlado a los recursos digitales.
- **Sistemas y Seguridad de Redes:** como las competencias de privacidad de datos, los sistemas y la seguridad de la red también son vistos como una "gran necesidad" por el 56% de las organizaciones. Esta habilidad es crucial para proteger la infraestructura crítica contra los ciberataques.
- **Seguridad de la Cadena de Suministro:** con el 48% identificándolo como una "gran necesidad", esta competencia refleja la creciente preocupación por garantizar que todos los eslabones de la cadena de suministro sean robustos frente a las amenazas cibernéticas.

Estas áreas reflejan una gran conciencia y necesidad de fortalecer las capacidades críticas de ciberseguridad.

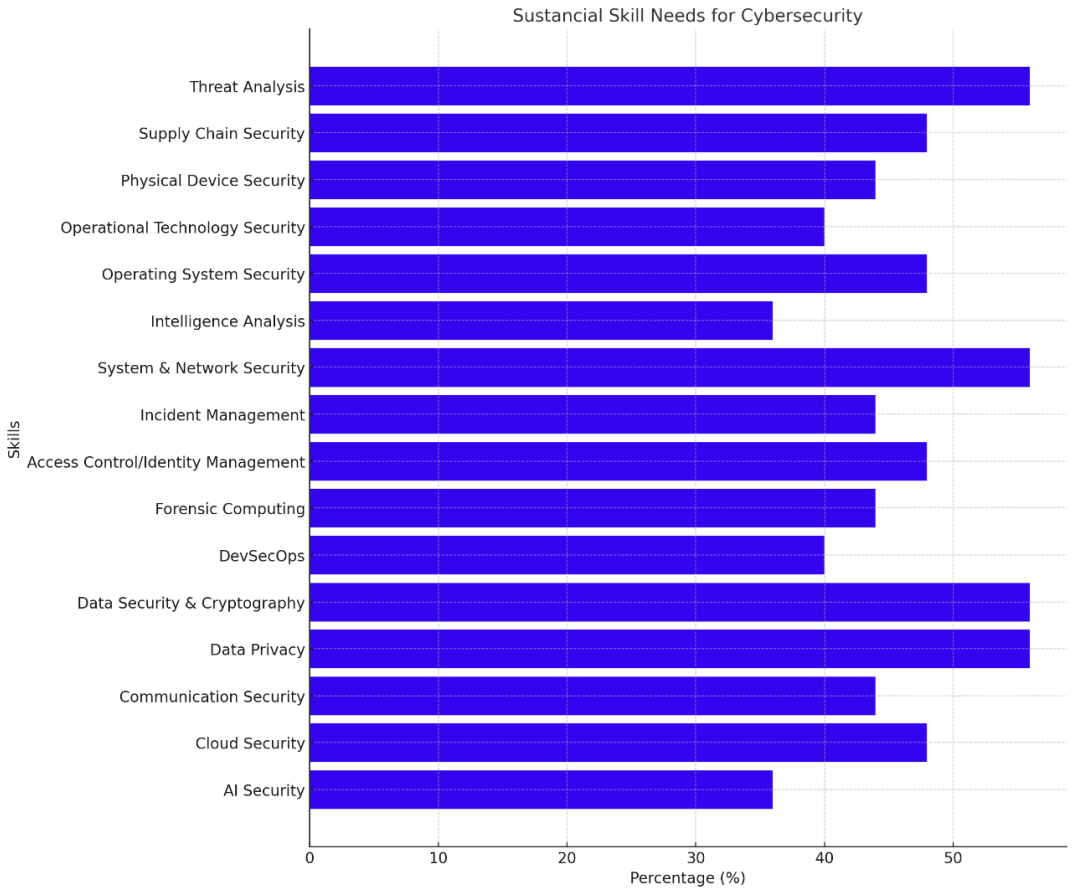

Gráfico2: Necesidades sustanciales de competencias en ciberseguridad

3.2.3 Formación

Importancia de las estrategias de formación en ciberseguridad

El 84% de las organizaciones indica una alta necesidad de formación, principalmente debido a desarrollos tecnológicos y a los cambios en la infraestructura organizacional. Sin embargo, el 40% enfrenta retrasos en esta formación capacitación, lo que podría comprometer su preparación contra las amenazas cibernéticas. Las estrategias de capacitación más valoradas incluyen:

- **Contratación y formación de personas:** el 69,57% lo considera "muy importante".
- **Formación y coaching en el puesto de trabajo:** también el 69,57% lo considera "muy importante".
- **Formación externa:** el 52,17% lo considera "muy importante".

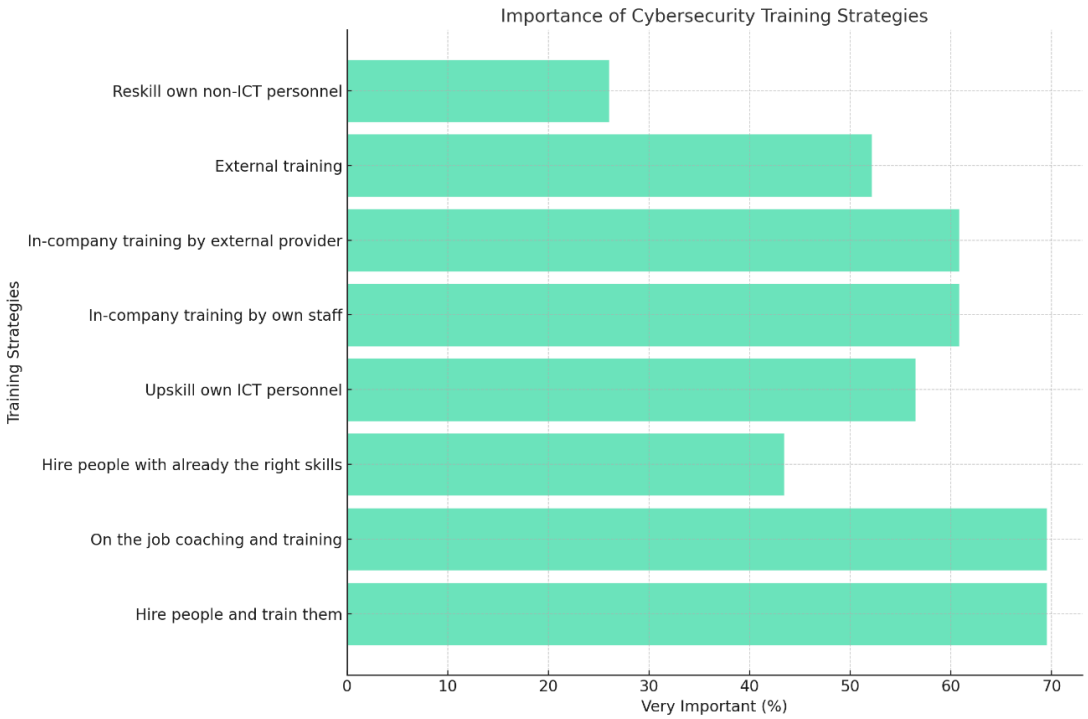

Gráfico3: Importancia de las estrategias de formación en ciberseguridad

Importancia de las certificaciones en ciberseguridad

Una parte significativa de las organizaciones ha enfatizado la necesidad crítica de certificaciones formales al contratar perfiles de ciberseguridad. Según los datos, las organizaciones están priorizando certificaciones y formación específicos para garantizar la preparación contra las amenazas cibernéticas.

- **Certificación formal relevante para un rol específico:** el 69.57% de las organizaciones califica este punto como "muy importante".
- **Licenciatura/maestría relevante para un rol específico:** otro 69,57% también considera este punto como "muy importante".
- **Educación formal relevante para un rol específico:** el 56.52% de las organizaciones considera esta calificación como "muy importante".
- **Certificados de participación en cursos:** el 47.83% los clasifica como "muy importantes".

Estos datos destacan la importancia de la educación formal y certificada para abordar los desafíos de ciberseguridad, ayudando a las organizaciones a armar una defensa sólida contra unas amenazas que están en constante evolución.

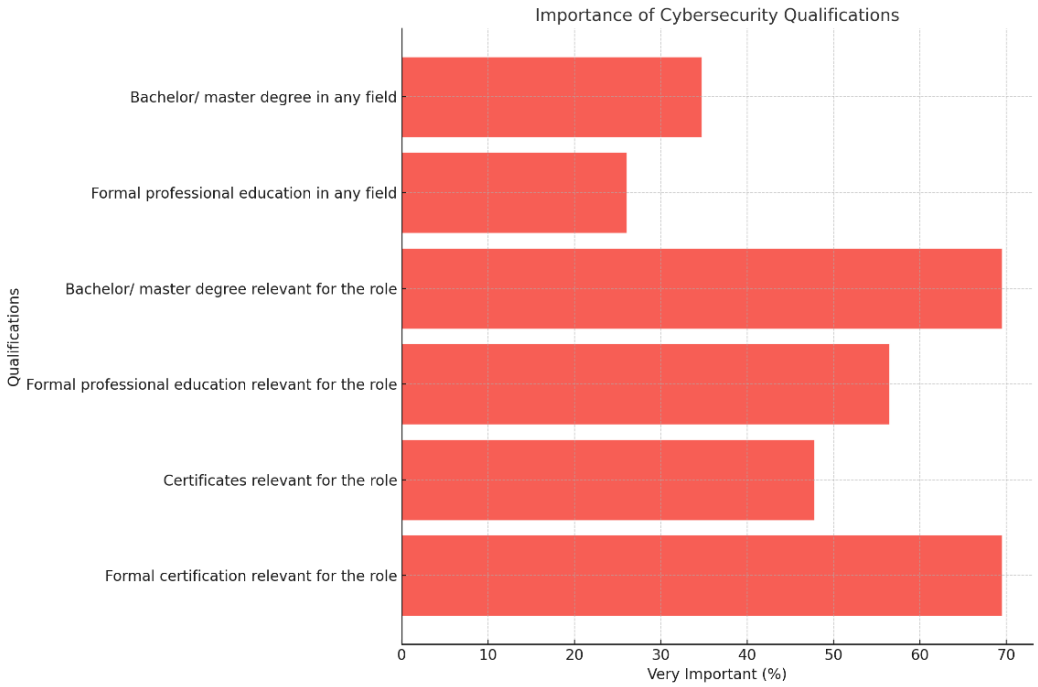

Gráfico4: Importancia de las cualificaciones de ciberseguridad

3.3 Conclusiones

El cuestionario destaca la necesidad urgente de roles especializados, competencias técnicas avanzadas y formación continua para abordar los desafíos de ciberseguridad en el entorno empresarial actual.

Los roles y necesidades de los profesionales se basan sobre todo en lenguajes de programación para la implementación, arquitectura y análisis de sistemas de ciberseguridad.

La creciente demanda de expertos en ciberseguridad con competencias técnicas (*hard skills*) y la alta valoración de competencias críticas reflejan la importancia de estar preparados para amenazas cibernéticas que están en constante evolución.

Además, aunque las empresas están avanzando en sus estrategias de ciberseguridad, los retrasos en la formación representan un riesgo significativo que debe abordarse con urgencia. Una planificación estratégica más sólida en materia de formación y desarrollo de competencias será crucial para mantener la competitividad y la seguridad a largo plazo.

4 Análisis de ofertas de empleo

4.1 Recopilación de datos

Para el análisis de ofertas de empleo se ha trabajado con las siguientes fuentes:

- **Glassdoor:** motor de búsqueda de empleo y experiencia laboral. Enlace: https://www.glassdoor.com/about/.
- **Indeed:** búsqueda de empleo. Enlace: https://www.indeed.com/.
- **LinkedIn:** red social orientada al uso empresarial, empresarial y laboral. Enlace: https://www.linkedin.com/.
- **Infosec Jobs**: búsqueda de empleo. Enlace: https://infosec-jobs.com/.
- **Himalayas:** aplicación de búsqueda de empleo para teletrabajo. Enlace: https://himalayas.app/jobs.

4.2 Resultados

Tabla 2: Principales resultados del análisis de ofertas de empleo

Ofertas de empleo (perfil ESCF)	Nº Ofertas de empleo (perfil ESCF)	Competencia	Nº Categoría de competencia
Implementador de Ciberseguridad (*Cybersecurity Implementer*)	469	Ciberseguridad (competencias técnicas o *hard skills*)	5333
Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*)	159	Tecnologías de la Información (competencias relacionadas con el rol profesional)	3449
Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*)	124	Competencias transversales (*soft skills*)	3145
Responsable de Ciberseguridad en Jurídico, Legal y Cumplimiento (*Cyber Legal, Policy and Compliance*)	81	Competencias organizativas	1648

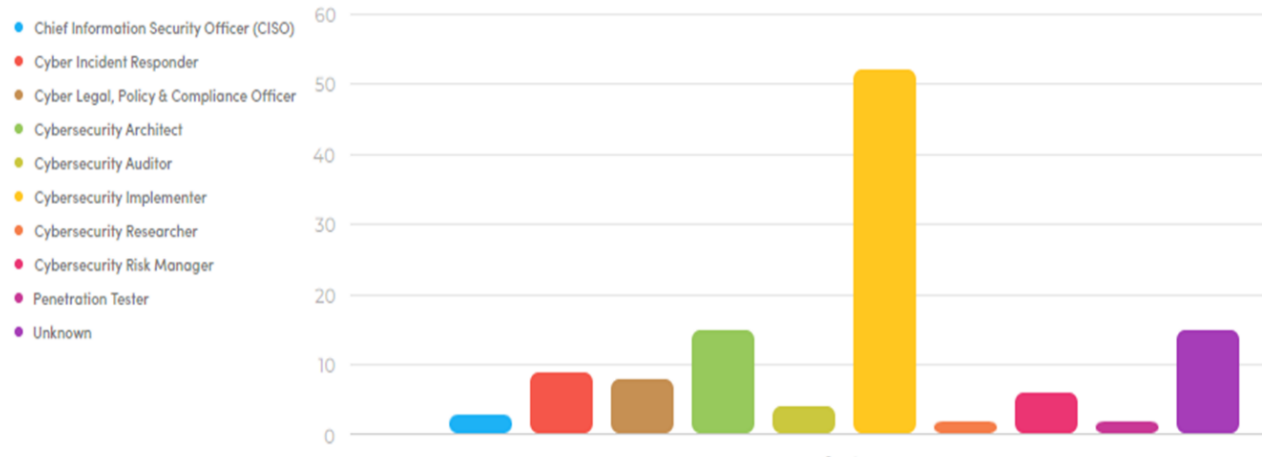

Gráfico5: Demanda de empleo por perfiles profesionales

Los resultados obtenidos para puestos de ciberseguridad según los roles descritos por ENISA, muestran 5 empresas principales que permanentemente ofrecen ofertas de empleo. Estas 5 empresas son las siguientes:

Tabla 3: Empresas que ofrecen permanentemente ofertas de empleo en ciberseguridad en España

EY	Proporciona servicios de auditoría, impuestos, asesoría en transacciones y consultoría.
Capgemini	Proporciona servicios de TI y consultoría, outsourcing y servicios profesionales.
Redes de Palo Alto	Empresa multinacional estadounidense de ciberseguridad.
Deloitte	Proporciona servicios de auditoría, consultoría, asesoría financiera, asesoría de riesgos, impuestos, legal y asesoría.
Grupo Santander	Multinacional financiera española.

4.3 Conclusiones

De acuerdo a los resultados obtenidos, se observa que España requiere profesionales de ciberseguridad en los roles donde más competencias técnicas se necesitan. Principalmente donde el conocimiento en programación, administración y configuración de redes, arquitectura de redes y sistemas de ciberseguridad, son la base para fortalecer los niveles de seguridad en empresas e instituciones.

Por ello, existe una necesidad evidente de más profesionales en los roles de Implementador de Ciberseguridad (*Cybersecurity Implementer*), Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*) y Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*), ya que estos puestos requieren un mayor conocimiento en tecnología de la información y los sistemas informáticos. Además, el manejo de lenguajes de programación y redes de datos como arquitectura e implementación son clave para poder solicitar estos trabajos.

En España, a diferencia de otros países participantes en el proyecto, se ha reforzado el rol de responsable de Seguridad de la Información (*Chief Information Security Officer-CISO*).

Integrando esta información con la obtenida en el análisis del mercado laboral, se evidencia que, efectivamente, a nivel nacional, roles como responsable de Seguridad de la Información (*Chief Information Security Officer-CISO*)

y Hacker Ético (*Ethical Hacker*) se cubren destacadamente a nivel privado; y en un nivel inferior en el ámbito público, ya que, aunque existen requisitos estrictos, es asequible para el mercado encontrar profesionales que cubran estos perfiles.

En contraste con lo anterior, existe una necesidad evidente de profesionales en roles donde se requieren competencias técnicas (*hard skills*), como Implementador de Ciberseguridad (*Cybersecurity Implementer*), Analistas de Amenazas de Ciberseguridad (*Cybersecurity Threat Analysts*) y Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*), lo que evidencia la necesidad de un mayor número de profesionales con experiencia en programación.

5 Investigación documental (oferta formativa)

5.1 Recopilación de datos

Los programas de formación en ciberseguridad en España analizados se han clasificado en dos grupos: títulos oficiales y títulos no oficiales. Se han estudiado los principales programas, considerando tanto la calidad del programa en sí como la institución impartidora. Además, se han analizado y comprobado los temas impartidos dentro de los programas, así como el número de horas y créditos asignados a cada materia.

Finalmente, se ha evaluado su adecuación con los roles de ENISA, que constituyen la base de este proyecto.

Desde el punto de vista de los roles de ENISA, se concluye que la oferta formativa se centra en roles como responsable de Seguridad de la Información (*Chief Information Security Officer-CISO*), responsable de Riesgos de Ciberseguridad (*Cybersecurity Risk Manager*) y Comprobador Prueba de Intrusión (*Penetration Tester*), siendo este último el perfil con mayores competencias técnicas requeridas.

Por otro lado, los programas no oficiales se centran en la adquisición de competencias más específicas desde el nivel técnico, como el hacking ético y la ciber inteligencia sobre amenazas.

5.2 Resultados

Se han analizado un total de 43 programas, de los cuales 30 son oficiales y 13 no oficiales. De los 30 programas oficiales, 21 se clasifican como maestrías y 9 como licenciaturas, centradas en la ciberseguridad, y en su mayoría ofrecidos online o en versión híbrida. Los programas oficiales son impartidos por las principales universidades de España. Sus programas son más bien generales y buscan cubrir diversos perfiles de interés dentro del entorno de ciberseguridad.

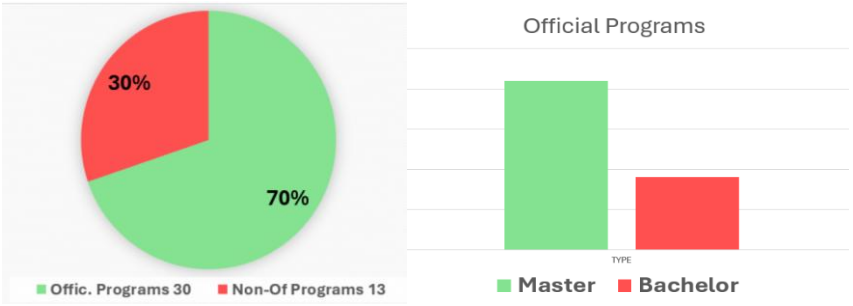

Gráfico6: Clasificación de Programas Formativos de Ciberseguridad en España

5.3 Conclusiones

Desde el punto de vista de los roles de ENISA, los contenidos de los 30 programas oficiales se centran en roles como responsable de Seguridad de la Información (*Chief Information Security Officer*-CISO), responsable de Riesgos de Ciberseguridad (*Cybersecurity Risk Manager*) y Comprobador Prueba de Intrusión (*Penetration Tester*).

Como se ha comentado anteriormente, los programas no oficiales se centran en la adquisición de competencias más específicas desde el nivel técnico, como el hacking ético y la ciber inteligencia sobre amenazas.

Una vez realizado este análisis y verificados los contenidos de la oferta formativa más relevante en España, se concluye que la formación en el ámbito de la ciberseguridad a nivel nacional requiere de un esfuerzo para mejorar las competencias de alto nivel requeridas en los roles de implementación, arquitectura y análisis de sistemas de ciberseguridad, fortaleciendo la formación en lenguajes de programación y diseño de nuevas tecnologías y sistemas para la ciberseguridad.

6 Panel de expertos

6.1 Recopilación de datos

El panel de expertos en ciberseguridad en España organizado en el marco del proyecto tuvo lugar el 18 de julio de 2024 y contó con la participación de destacados profesionales en el campo. El objetivo del panel fue explorar el estado actual y las perspectivas futuras de la ciberseguridad, con un enfoque particular en roles, competencias y capacitación necesarios para fortalecer este campo.

El panel estaba compuesto por los siguientes expertos:

- 1 director de Marketing y Comunicaciones de un proveedor de ciberseguridad.
- 1 ingeniero de telecomunicaciones y experto en ciberseguridad de un centro de investigación e innovación sin ánimo de lucro.
- 1 director de Operaciones de una consultora especializada en transformación digital y optimización de procesos.
- 1 CEO y experto en ciberseguridad de una empresa de ciberseguridad.
- 1 ingeniera industrial y presidenta de una organización sin ánimo de lucro enfocada en promover y aumentar la participación de las mujeres en el campo de la ciberseguridad.
- 1 CIO/CTO de una asociación sin ánimo de lucro que promueve el desarrollo de un ecosistema blockchain.
- 1 ingeniero informático y experto en ciberseguridad de una institución de educación superior.
- 1 director de una asociación empresarial sin ánimo de lucro que representa a la industria tecnológica y digital.

La reunión duró dos horas y tuvo lugar online, lo que permitió una participación dinámica y accesible por parte de todos los expertos.

Con el objetivo de abordar de manera integral los desafíos y necesidades actuales en el campo de la ciberseguridad, el panel se estructuró en dos mesas de debate:

1. **Industria:** se centró en explorar las necesidades y desafíos específicos a los que se enfrentan las empresas en ciberseguridad, incluida la demanda de profesionales, las competencias requeridas y la interacción con el sector educativo.

2. **Ecosistemas:** se centró en analizar la importancia de la sensibilización y la cultura de la ciberseguridad a nivel social, así como la colaboración entre diversos agentes para fomentar un entorno digital más seguro y resiliente.

Esta configuración permitió una discusión más enfocada y profunda en cada área, facilitando la identificación de problemas y soluciones específicas desde diferentes perspectivas, pero complementarias entre sí.

Se abordaron tres temas centrales:

- Roles en ciberseguridad.
- Competencias necesarias en los profesionales de ciberseguridad.
- Formación de estos profesionales.

A continuación, se explican los resultados cualitativos de las discusiones, y se indican asimismo citas que reflejan el consenso entre los participantes.

6.2 Resultados

1. **Falta de expertos:** hay una escasez significativa de profesionales con competencias específicas en ingeniería de desarrollo, ingeniería industrial y programación. Esta escasez ha llevado a muchas empresas a buscar talento extranjero para satisfacer estas necesidades críticas. Como destaca el CEO y experto en ciberseguridad de una empresa de ciberseguridad:

«Hay una clara falta de expertos en ingeniería de desarrollo. A menudo tenemos que confiar en ingenieros de otros países para satisfacer necesidades críticas.

Adicionalmente, el experto en ciberseguridad de la universidad expresa:

"Hay una escasez de implementadores, arquitectos de ciberseguridad y expertos en respuesta a incidentes".

2. **Necesidad de formación específica:** se hace hincapié en la importancia de fortalecer la formación en áreas críticas como la programación y la aplicación de sistemas. Esta falta de formación especializada limita la capacidad de las organizaciones para desarrollar y mantener infraestructuras de seguridad sólidas. Por otra parte, el director de Operaciones de la consultora añade:

"Es crucial que la formación de los profesionales incluya no solo competencias técnicas sino también un entendimiento claro de las regulaciones de ciberseguridad, algo que muchos CISO todavía no dominan totalmente".

3. **Desafíos en el sector público:** las administraciones públicas, especialmente las más pequeñas, se enfrentan a grandes retos en el cumplimiento de las normas de seguridad debido a la falta de recursos y conocimientos. Esto crea vulnerabilidades significativas en la protección de datos y servicios públicos. El director de Operaciones de la consultora expresa esta preocupación:

"Las pequeñas administraciones carecen de los recursos y conocimientos necesarios para cumplir con las normas de seguridad, dejándolas expuestas a vulnerabilidades", agregó, "en términos de estructura, gobernanza y hoja de ruta, aún queda mucho por hacer".

6.2.1 Roles profesionales

Se requieren profesionales con competencias de alto nivel en ciberseguridad, ya que la evolución y el crecimiento constante de las tecnologías y, por lo tanto, de las amenazas cibernéticas, requieren una mayor preparación y conocimiento en ciberseguridad.

De hecho, se necesitan más profesionales en los siguientes perfiles, por orden de importancia:

1. Implementador de Ciberseguridad (*Cybersecurity Implementer*).

2. Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*).

3. Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).

6.2.2 Competencias

Refuerzo de la estructura de ciberseguridad:

1. **Marco regulatorio:** se propone la creación de una agencia española de ciberseguridad para estandarizar y normalizar directrices que faciliten la implementación de políticas de ciberseguridad. Un marco regulatorio sólido es esencial para garantizar que las prácticas de ciberseguridad se implementen de manera consistente en todo el país. El director de Operaciones de la consultora sugiere:

"Promover un marco regulatorio y crear una autoridad de supervisión para estandarizar y normalizar las directrices".

2. **Colaboración público-privada:** la colaboración entre la administración pública y el sector privado se considera fundamental para mejorar la aplicación de las medidas de ciberseguridad. Esta cooperación es crucial para compartir conocimientos, recursos y buenas prácticas. El experto en ciberseguridad de la universidad enfatiza:

"Es necesaria una mayor integración entre el Estado, la educación y el sector privado para crear una sociedad preparada para esta era digital".

3. **Dinamismo y adaptación:** la rápida evolución tecnológica requiere una regulación ágil y flexible. Además, se necesita una mayor colaboración entre universidades y empresas para garantizar que la formación y las prácticas de ciberseguridad evolucionen junto con las necesidades del mercado. El CEO y experto en ciberseguridad de una empresa de ciberseguridad comenta:

«Es importante el dinamismo en la regulación y la adaptación constante a los cambios tecnológicos».

6.2.3 Formación

Rol del sector educativo:

1. **Facilitar la entrada en el mercado laboral:** es esencial que los programas de Formación Profesional (FP) incluyan prácticas que permitan a los estudiantes adquirir experiencia en entornos de trabajo reales. Estas prácticas son clave para que los nuevos profesionales desarrollen las competencias necesarias para enfrentarse a los desafíos actuales de ciberseguridad. El experto en ciberseguridad del centro de investigación e innovación sin ánimo de lucro destaca:

"Los estudiantes que se gradúan en programas vocacionales y universitarios necesitan más oportunidades para aplicar lo que han aprendido. Es crucial que tengan acceso a programas de prácticas para desarrollar estas competencias.

2. **Colaboración universidad-industria:** se hace hincapié en la importancia de que las instituciones de educación superior se acerquen a las empresas para adaptar la formación académica a las necesidades prácticas del mercado laboral. Esta colaboración garantizaría que los estudiantes estén mejor preparados para satisfacer las demandas específicas del sector. El CEO y experto en ciberseguridad de una empresa de ciberseguridad enfatiza:

«Las instituciones de educación superior deben acercarse a las empresas. La ciberseguridad es un campo muy cerrado, donde las empresas son reacias a compartir sus conocimientos. Esto dificulta que los nuevos profesionales adquieran la experiencia práctica que tanto se necesita».

3. **Programas interdisciplinares:** la creación de títulos que integren disciplinas como el derecho y la inteligencia artificial se considera una tendencia necesaria. Estos programas requieren una estrecha colaboración entre la industria y la academia para desarrollar un plan de estudios que combine el conocimiento técnico con una comprensión de las implicaciones legales y éticas. El director de Operaciones de la consultora menciona:

«Se están creando grados que combinan diversas disciplinas, como la jurídica y la IA. La industria y el mundo académico deben colaborar estrechamente».

Ecosistemas: concienciación en ciberseguridad y cibercultura

1. **Divulgación de la ciberseguridad:** se destaca la necesidad de promover una cultura de ciberseguridad en todos los niveles, no solo en el ámbito empresarial, sino también en el social. La educación y la

sensibilización en materia de ciberseguridad son esenciales para que todos los actores comprendan y asuman sus responsabilidades. El CIO/CTO de la asociación sin ánimo de lucro señala:

"Es vital evangelizar sobre la ciberseguridad y crear conciencia en las empresas sobre la importancia de implementar una cultura cibernética en todos los niveles".

2. **Responsabilidad compartida:** la ciberseguridad es una responsabilidad colectiva. Es crucial transmitir este mensaje para crear conciencia sobre los riesgos de ciberseguridad y las mejores prácticas, tanto profesional como personalmente.

3. **Diversidad:** una cuestión crítica que no se aborda en la encuesta es la diversidad dentro del sector. La falta de diversidad representa un área de mejora en futuros proyectos, ya que un enfoque más inclusivo podría mejorar la innovación y la eficacia en las estrategias de ciberseguridad. La ingeniera industrial, presidenta y fundadora de una organización sin ánimo de lucro critica:

"La diversidad no se aborda en la encuesta, que es un área que debemos abordar en futuros proyectos".

6.3 Conclusiones

1. **Escasez de profesionales cualificados:** sigue existiendo una escasez de profesionales cualificados, y es fundamental cerrar el ciclo de formación con una mayor inserción laboral. El experto en ciberseguridad del centro de investigación e innovación sin ánimo de lucro concluye:

"Debemos facilitar la entrada de jóvenes profesionales en el mercado laboral a través de prácticas laborales, para que no se encuentren sin empleo después de su formación".

2. **Integración estado-educación-empresa:** es vital que estos tres pilares trabajen juntos en preparar a la sociedad para los desafíos del ciberespacio. La colaboración y la alineación de objetivos entre estos sectores son esenciales para crear un entorno seguro y resiliente en la era digital.

3. **Análisis DAFO del sector:** se sugiere llevar a cabo un análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades) para abordar los retos de ciberseguridad en todos los niveles de la sociedad. Este análisis permitiría identificar áreas prioritarias y diseñar estrategias efectivas para fortalecer la ciberseguridad.

7 Conclusiones

Al integrar y correlacionar toda la información recopilada durante el análisis, se han podido destacar las fortalezas, debilidades, oportunidades y amenazas de la ciberseguridad en España.

Fortalezas:

La estrategia nacional de ciberseguridad está alineada con la regulación, la innovación y la implementación de las tecnologías actuales y futuras. Esto incluye a todos los niveles de la sociedad e instituciones.

La educación y formación en ciberseguridad es amplia y variada y es posible acceder a la misma online o presencialmente. Los títulos universitarios y de especializaciones concretas constituyen la principal vía para la adquisición de conocimientos en ciberseguridad, y existen planes y becas que permiten a los interesados acceder a la formación con mayor facilidad.

La empresa privada posee una buena capacidad tecnológica para la ciberseguridad. De la misma manera, el sector de la defensa tiene un alto nivel de capacidades de ciberdefensa.

El nivel de implantación e innovación de nuevas y futuras tecnologías de la información es muy competente, permitiendo la creación de nuevos perfiles y puestos de trabajo, y manteniendo un flujo constante de solicitudes de empleo en el sector de la ciberseguridad.

Debilidades:

La mayor debilidad consiste en la falta de profesionales de ciberseguridad, especialmente de aquellos que tienen capacidades para ocupar puestos donde se requieren competencias técnicas. Esto está alineado con el hecho de que los programas educativos no se centran en la formación de temas específicos y de alto nivel en el área.

Aunque la remuneración de los profesionales de ciberseguridad en España es buena, se evidencia que es más baja que en otros países, lo que genera una fuga de profesionales de ciberseguridad a otros países de la región.

El sector público es el eslabón más débil de la cadena, y, aunque cuenta con elementos que lo sustentan, es el área donde más se refleja la necesidad de profesionales de ciberseguridad y de implementación de sistemas y tecnologías.

Oportunidades:

El nivel de innovación y de progreso en la educación y la formación en ciberseguridad a nivel nacional es muy alto, lo que permite mantener y generar mejores profesionales y conocer las necesidades en el entorno digital, y por tanto en ciberseguridad.

La empresa privada ha dado pasos importantes en la innovación de la ciberseguridad, ya que existen grandes empresas con excelentes capacidades tecnológicas con capacidad para dar servicio a otros actores en el entorno nacional.

Amenazas:

El mayor riesgo observado es la innovación constante y el avance de la ciberdelincuencia, así como todas las amenazas potenciales que están creciendo y pueden aprovecharse de las debilidades descritas anteriormente.

Otra amenaza es la fuga de profesionales con sólidos conocimientos en ciberseguridad a otros países de la región.

7.1 Roles profesionales

Aunque a nivel nacional se necesitan profesionales en todos los puestos en el área de ciberseguridad, este análisis demuestra que esta necesidad se acentúa en los siguientes roles:

1. Implementador de Ciberseguridad (*Cybersecurity Implementer*).

2. Arquitecto de Ciberseguridad (*Cybersecurity Arquitect*).

3. Respuesta ante Incidentes Cibernéticos (*Cyber Incident Responder*).

Se requieren profesionales con conocimiento en lenguajes de programación y competencias técnicas en implementación y arquitectura de sistemas de ciberseguridad.

Los perfiles como responsable de Seguridad de la Información (*Chief Information Security Officer-CISO)*, Hacker Ético (*Ethical Hacker*) o ciber inteligencia sobre amenazas están cubiertos en un nivel satisfactorio, principalmente el perfil CISO.

El sector público en España precisa de una mejora en todos los perfiles relacionados con las tecnologías de ciberseguridad.

Por último, queda patente que la escasez de expertos en estas áreas lleva a las empresas a buscar talento en el extranjero.

7.2 Competencias

Los programas de formación en ciberseguridad oficiales y no oficiales requieren un enfoque especial, fortaleciendo el aprendizaje de competencias técnicas, principalmente en lenguajes de programación para la ciberseguridad.

La implementación de la ciberseguridad, la arquitectura y la respuesta a incidentes son requisitos específicos en los programas de ciberseguridad, centrándose en las competencias técnicas.

Es necesario fortalecer el sector público con más profesionales en Seguridad de la Información (*Chief Information Security Officer-CISO)* y en ciber inteligencia sobre amenazas, ya que es aquí donde reside la fortaleza en España.

Se necesita un conocimiento y manejo específicos de la ley y las políticas públicas. Prueba de ello es la sugerencia que se hizo en el panel de expertos sobre un marco normativo sólido. Este conocimiento podría incluirse dentro de las nuevas competencias de los profesionales de la ciberseguridad.

7.3 Formación

Se requieren programas formativos en el área de ciberseguridad centrados en los siguientes campos:

- Lenguajes de programación.
- Implementación de sistemas.
- Arquitectura de sistemas.

Se requiere fortalecer los programas que ya existen e introducir otros nuevos, centrándose en áreas como la programación para la ciberseguridad, el desarrollo de sistemas de ciberseguridad y tecnologías innovadoras para

defender, responder y contrarrestar las amenazas cibernéticas. Estos programas deben facilitar a los recién graduados la entrada al mercado laboral. También es necesario adaptar o crear programas de formación hacia un enfoque más interdisciplinario.

Por último, las instituciones de educación superior y de formación deben colaborar más estrechamente con el sector privado, para garantizar que los estudiantes estén mejor preparados para satisfacer las demandas de la industria.

8 Referencias

- CCN-CERT. (2023). *Enfoque de la inteligencia artificial y la ciberseguridad: Informe sobre las mejores prácticas.*
- Deloitte. (2023). *El estado de la ciberseguridad en España.*
- Disruptivo. (2023). *Informe sobre la situación de la ciberseguridad 2023: Tendencias, retos y oportunidades.*
- ENISA (2022) Perfiles de funciones del Marco Europeo de Capacidades en Ciberseguridad — ENISA (europa.eu)
- Foro Nacional de Ciberseguridad. (2023). *Foro Nacional de Ciberseguridad. Motor de la Colaboración Público-Privada.*
- Foro Nacional de Ciberseguridad. (2021). *Informe sobre la cultura de la ciberseguridad en España.*
- Fundación Alternativas. (2023). *IV Informe sobre Ciencia y Tecnología en España: Tendencias, retos y oportunidades en ciberseguridad.*
- GlobalData (en inglés). (2023). *España: Tendencias laborales relacionadas con la ciberseguridad (octubre de 2023 - enero de 2024).*
- INCIBE (en inglés). (2022). *Análisis y Diagnóstico del Talento en Ciberseguridad en España.* Instituto Nacional de Ciberseguridad.
- Inteligencia de Mordor. (2024). *Mercado de ciberseguridad en España Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029).*
- Revista Red Seguridad (en inglés). (2023). *Cinco cosas que los profesionales de la ciberseguridad deben tener en cuenta en 2024.*
- Gobiernode España. (2022). *Digital Spain 2026* (en inglés). Ministerio de Asuntos Económicos y Transformación Digital.
- Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad: Una prioridad, un reto y un compromiso para todos.*
- UNE. (n.d.). *La normalización contribuye a prevenir los ciberataques y a proteger las comunicaciones.* Asociación Española de Normalización.

9 Anexos

9.1 Anexo 1. Resumen de la investigación documental (demanda)

Nombre	Publicado en	Autores	Año	Idioma	Enlace	Tema(s) clave	Resumen
Estrategia Nacional de Ciberseguridad	PCI/487/2019, de 26 de abril	Departamento de Seguridad Nacional	2019	español	https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019	Las amenazas y desafíos del ciberespacio. Propósito, principios y objetivos para la ciberseguridad	La Estrategia Nacional de Ciberseguridad define objetivos, plasma los principios, identifica a los diferentes actuales y potenciales amenazas en el ciberespacio y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además define el modelo de gobernanza para la implementación, seguimiento y evaluación de la ciberseguridad nacional de España.
Estrategia Nacional de Ciberseguridad	PCI/487/2019, 26 de abril	Departamento de Seguridad Nacional	2019	inglés	https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019	Las amenazas y desafíos del ciberespacio. Propósito, principios y objetivos para la ciberseguridad	La Estrategia Nacional de Ciberseguridad define objetivos, plasma los principios, identifica a los diferentes actuales y potenciales amenazas en el ciberespacio y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad; además define el modelo de gobernanza para la implementación, seguimiento y evaluación de la ciberseguridad nacional de España.
Estrategia Nacional de Ciberseguridad. España 2019 Una prioridad, un reto y un compromiso para todos.	26 de abril de 2023	Manuel Sánchez Gómez-Merelo	2023	español	https://www.aesseguridad.es/news/55/Noticia_03_Estrategia_Nacional_Ciberseguridad.pdf	Resumen ejecutivo estrategia nacional de ciberseguridad 2019	Resumen de la Estrategia, guía de bases generales, El documento se estructura en cinco capítulos. 1, El ciberespacio, más allá de un espacio común global, 2, «Las amenazas y desafíos en el ciberespacio, 3. Propósito, principios y objetivos para la ciberseguridad, 4. Líneas de acción y medidas, 5. «La ciberseguridad en el Sistema de Seguridad Nacional.

Nombre	Publicado en	Autores	Año	Idioma	Enlace	Tema(s) clave	Resumen
Análisis y Diagnóstico del Talento en Ciberseguridad en España	22 de marzo	INCIBE	2022	español	https://files.incibe.es/incibe/talento/INCIBE_InformeCompleto_DIAG.pdf	Plan España digital 2025	Análisis y Diagnóstico del Talento de Ciberseguridad en España, que identifica de manera detallada la situación actual, al tiempo que ofrece escenarios futuros para ayudar a la industria y las administraciones públicas en la búsqueda de soluciones para la identificación, generación y transformación de talento.
IV Informe sobre la Ciencia y Tecnología en España	2023	SARA DEGLI-ESPOSTI Y MANUEL SUÁREZ ROMÁN	2023	español	https://digital.csic.es/bitstream/10261/310469/3/Investigaci%c3%b3n_ciberseguridad_Espa%c3%b1a.pdf	I+D+i en ciberseguridad en España,	Análisis centrado en analizar indicadores de excelencia investigadora, captación de recursos económicos y oferta formativa entidades (universidades, OPI o centros privados de investigación) en los que se ha identificado investigadores que trabajen en las áreas estrictamente relacionadas con la I+D+i en ciberseguridad
El estado de la ciberseguridad en España	2023	Deloitte	2023	español	https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html	CISO	Análisis del estado de la ciberseguridad desde la visión de los CISO y responsables de la ciberseguridad en España, toma muestra de empresas privadas y sus experiencias en ciberseguridad a nivel nacional.
CIBERSEGURIDAD Informe de situación 2023	2023	Disruptivo.	2023	español	https://ptedisruptive.es/wp-content/uploads/2023/12/Informe-situación-ciberseguridad-2023_compressed.pdf	Tendencias, retos y oportunidades en ciberseguridad	Estudio resumen de la ciberseguridad en España, las tendencias y las amenazas cibernéticas, asimismo, estado actual de la implementación de la estrategia de ciberseguridad.
Foro Nacional de Ciberseguridad.	actualizado Junio 2023	Departamento de Seguridad Nacional	2021	español	https://foronacionalciberseguridad.es/index.php/documentacion/publico/119-foro-nacional-de-ciberseguridad-2023/file	Colaboración público-privada en ciberseguridad	Actualización del informe de 2021, análisis y informe para actualizar y proponer iniciativas para desarrollar la Estrategia Nacional de Ciberseguridad a través de sinergias público-privadas que permitan dotar de una mayor protección a la sociedad española en toda su amplitud.

Nombre	Publicado en	Autores	Año	Idioma	Enlace	Tema(s) clave	Resumen
APROXIMACIÓN A LA INTELIGENCIA ARTIFICAL Y LA CIBERSEGURIDAD	23 de octubre	CCN-CERT	2023	español	https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/7190-ccn-cert-bp-30-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad/file.html	Tendencias emergentes, Formación continua	Informe de análisis de la irrupción de la Inteligencia artificial, en la ciberseguridad.
CINCO COSAS A TENER EN CUENTA POR LOS PROFESIONALES DE LA CIBERSEGURIDAD DURANTE 2024	25/03/2024	Revista Red Seguridad	2024	español	https://www.redseguridad.com/	Tendencias futuras	Artículo en relación a las competencias de los profesionales de la ciberseguridad y las tendencias futuras

9.2 Anexo 2. Programas de formación (investigación documental - oferta)

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Máster Universitario en Ciberseguridad	Ciberseguridad defensiva	EQF7 (máster)	Universidad de Alcalá	Pública	https://www.uah.es/es/estudios/Ciberseguridad/	Grado	47	20	Oficial 60 ECTS completos + 30 ECTS parciales
España	Máster Universitario Online en Ciberseguridad	Gestión de la ciberseguridad	EQF7 (máster)	Universidad Alfonso X El Sabio	Privada	https://www.uax.com/titulaciones/master-en-ciberseguridad-online	Grado	10	40	Oficial 60 ECTS Online
España	Máster Universitario en Ciberseguridad	Ciberseguridad, seguridad de la información	EQF7 (máster)	Universidad de Alicante	Pública	https://web.ua.es/es/masteres/ciberseguridad/master-universitario-en-ciberseguridad.html	Grado	147	20	Oficial 60 ECTS Online
España	Máster Universitario en Seguridad Informática (Ciberseguridad)	Seguridad de la información	EQF7 (máster)	Universidad de Cádiz	Pública	https://esingenieria.uca.es/docencia/masteres/master-en-ciberseguridad-datos-informacion/	Grado	10	30	Oficial 60 ECTS Presencial
España	Máster Universitario en Ciberseguridad	Ciberseguridad defensiva	EQF7 (máster)	Universidad Camilo José Cela	Privada	https://www.ucjc.edu/master/ciberseguridad/	Grado	147	50	Oficial 60 ECTS Online
España	Máster Universitario en Ciberseguridad	Analista de Ciberseguridad	EQF7 (máster)	Universidad Carlos III de Madrid	Pública	https://www.uc3m.es/master/ciberseguridad	Grado	96	60	Oficial 60 ECTS Presencial
España	Graduado/a en Ciberseguridad	Seguridad de la información y ciberseguridad	EQF6 (licenciatura)	Universidad de Euneiz	Privada	https://www.euneiz.com/grados-universitarios/grado-ciberseguridad/	Grado	156	40	Oficial 240 ECTS Presencial
España	Graduado/a en Ingeniería de la Ciberseguridad	Seguridad de la información y ciberseguridad	EQF6 (licenciatura)	Universidad Europea de Madrid	Privada	https://universidadeuropea.com/grado-ciberseguridad-madrid/	Grado	18		Oficial 240 ECTS Presencial

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones	Gestión de la ciberseguridad	EQF7 (máster)	Universidad Europea de Madrid	Privada	https://universidadeuropea.com/master-ciberseguridad-madrid/	Grado	10	35	Oficial 60 ECTS Presencial
España	Graduado/a en Gestión de la Ciberseguridad	Hacking ético	EQF6 (licenciatura)	Universidad Francisco de Vitoria	Privada	https://www.ufv.es/estudiar-grado-gestion-ciberseguridad-madrid/	Grado	6	60	Oficial 240 ECTS Presencial
España	Graduado/a en Ciberseguridad	Seguridad de la información y ciberseguridad	EQF6 (licenciatura)	Universidad Internacional de La Rioja	Privada	https://www.unir.net/ingenieria/grado-ciberseguridad/	Grado	99	1200	Oficial 240 ECTS Híbrido
España	Máster Universitario en Ciberseguridad	Seguridad de la información y ciberseguridad	EQF7 (máster)	Universidad Internacional de La Rioja	Privada	https://www.unir.net/ingenieria/master-seguridad-informatica/	Grado	8	750	Oficial 240 ECTS Online
España	Máster Universitario en Ciberseguridad	Seguridad de la información	EQF7 (máster)	Internacional Isabel I de Castilla	Privada	https://www.ui1.es/oferta-academica/master-en-ciberseguridad	Grado	47		Oficial 60 ECTS Online
España	Máster Universitario en Ciberseguridad	Gestión de la ciberseguridad	EQF7 (máster)	Universidad Internacional Valenciana	Privada	https://www.upv.es/titulaciones/MUCC/	Grado	19	30	Oficial 90 ECTS Híbrido
España	Máster Universitario en Seguridad Informática	Seguridad de la información	EQF7 (máster)	Universidad de Jaén	Pública	https://www.ujaen.es/estudios/oferta-academica/masteres/master-universitario-en-seguridad-informatica	Grado	47	30	Oficial 60 ECTS Híbrido
España	Máster Universitario en Ciberseguridad e Inteligencia de Datos	Gestión de la ciberseguridad	EQF7 (máster)	Universidad de La Laguna	Pública	https://www.ull.es/masteres/ciberseguridad-inteligencia-datos/	Grado	19	30	Oficial 60 ECTS Híbrido

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Máster Universitario en Investigación en Ciberseguridad	Análisis Forense Digital	EQF7 (máster)	Universidad de León	Pública	https://www.unileon.es/estudiantes/oferta-academica/masteres/mu-investigacion-ciberseguridad-online	Grado	3	60	Oficial 60 ECTS Online
España	Graduado/a en Ciberseguridad e Inteligencia Artificial	Seguridad de la información y ciberseguridad	EQF6 (licenciatura)	Universidad de Málaga	Pública	https://www.uma.es/grado-en-ciberseguridad-e-inteligencia-artificial/	Grado	21	65	Oficial 240 ECTS Presencial
España	Máster de formación permanente online en ciberseguridad	Seguridad de la información	EQF7 (máster)	Universidad de Mondragón	Privada	https://www.mondragon.edu/cursos/es/master-ciberseguridad	Grado	10	50	Oficial 60 ECTS Online
España	Máster Universitario en Ciberseguridad	Ciberdefensa	EQF7 (máster)	Universidad de Murcia	Pública	https://www.um.es/web/estudios/masteres/ciberseguridad	Grado	10	50	Oficial 90 ECTS Online
España	Máster Universitario en Ciberseguridad	Hacking ético	EQF7 (máster)	UNED	Pública	https://www.uned.es/universidad/inicio/estudios/masteres/master-universitario-en-ciberseguridad.html	Grado	47	75	Oficial 60 ECTS Híbrido
España	Máster Universitario en Ciberseguridad y Privacidad	Protección de datos	EQF7 (máster)	Universitat Oberta de Catalunya	Privada	https://www.uoc.edu/es/estudios/masters/master-universitario-ciberseguridad-privacidad	Grado	83		Oficial 60 ECTS Online
España	Máster Universitario en Ciberseguridad	Seguridad de la información	EQF7 (máster)	Universidad Politécnica de Catalunya	Pública	https://www.upc.edu/ca/masters/ciberseguridad	Grado	20	44	Oficial 60 ECTS Presencial

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Máster Universitario en Ciberseguridad	Seguridad de la información y ciberseguridad	EQF7 (máster)	Universidad Politécnica de Madrid	Pública	https://www.upm.es/Estudiantes/Estudios_Titulaciones/Estudios_Master/Programas?id=9.19&fmt=detail	Grado	20	25	Oficial 60 ECTS Presencial
España	Máster Universitario en Ciberseguridad y Ciberinteligencia	Ciberseguridad y Ciberinteligencia	EQF7 (máster)	Universidad Politécnica de Valencia	Pública	https://www.upv.es/titulaciones/MUCC/indexc.html	Grado	9	30	Oficial 90 ECTS Híbrido
España	Graduado/a en Ingeniería de la Ciberseguridad	Ciberseguridad, seguridad de la información	EQF6 (licenciatura)	Universidad Rey Juan Carlos	Pública	https://www.urjc.es/universidad/calidad/3100-ingenieria-de-la-ciberseguridad	Grado	23	60	Oficial 240 ECTS Presencial
España	Máster Universitario en Ingeniería de la Seguridad Informática e IA	Ciberseguridad, seguridad de la información	EQF7 (máster)	Universidad Rovira i Virgili	Pública	https://www.iu.org/master/ciberseguridad/	Grado	16		Oficial 120 ECTS Online
España	Graduado/a en Ingeniería de la Ciberseguridad	Ciberseguridad, seguridad de la información	EQF6 (licenciatura)	Universidad de San Jorge	Privada	https://www.usj.es/estudios/grados/ingenieria-ciberseguridad	Grado	23	50	Oficial 240 ECTS Presencial
España	Máster Universitario en Ciberseguridad	Ciberseguridad, seguridad de la información	EQF7 (máster)	Universidad de Vigo	Pública	https://www.uvigo.gal/es/node/247124	Grado	89	0	Oficial 90 ECTS Presencial
España	Máster en Ciberseguridad (Presencial con Deloitte)	Hacking ético	EQF7 (máster)	IMF Smart Education	Privada	https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica-presencial	Grado			No oficial Presencial

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Máster Ciberseguridad en Hacking Ético: Redes CCNA + CiberOps + Fortinet	Hacking ético	EQF7 (máster)	Tajamar	Privada	https://fpprofessionaleducation.tajamar.es/ciberseguridad-en-redes/	Grado			No oficial Presencial
España	Hacker ético certificado	Hacking ético	EQF5 (CFGS de FP)	IT Institute	Privada	https://es.it-institute.org/ceh-certified-ethical-hacker/	Certificado			No oficial Online
España	Ciberseguridad en Redes: CCNA + CyberOps + Fortinet	Hacking ético	EQF5 (CFGS de FP)	Tajamar	Privada	https://fpprofessionaleducation.tajamar.es/ciberseguridad-en-redes/	Diploma			No oficial Híbrido
España	Operaciones de ciberseguridad - Cisco Certified CyberOps Associate (CBROPS)	Ciberdefensa	EQF5 (CFGS de FP)	PUE	Privada	https://www.pue.es/cursos/cisco/200-201-cyberops-associate	Certificado			No oficial
España	Master Propio en Datos, Redes Complejas & Ciencias de Ciberseguridad	Gestión de la ciberseguridad	EQF7 (máster)	Universidad Rey Juan Carlos	Pública	https://www.urjc.es/component/k2/4363-data-complex-networks-cybersecurity-sciences	Grado		50	No oficial Híbrido
España	Gestión de la Ciberseguridad	Gestión de la ciberseguridad	EQF5 (CFGS de FP)	Universidad Francisco de Vitoria	Privada	https://www.ufv.es/plan-de-estudios-grado-en-gestion-de-la-ciberseguridad/	Grado			No oficial
España	Ingeniería de la Ciberseguridad	Ciberseguridad, seguridad de la información	EQF6 (licenciatura)	Universidad Rey Juan Carlos	Pública	https://www.urjc.es/universidad/calidad/3100-ingenieria-de-la-ciberseguridad	Diploma		60	No oficial 240 ECTS Presencial

País	Título	Especialización	Nivel	Institución	Tipo de institución	Enlace	Certificación	Nº egresados (2021-22)	Nº alumnos potenciales	Otra información
España	Bootcamp de ciberseguridad	Hacking ético	EQF5 (CFGS de FP)	Ironhack	Privada	https://www.ironhack.com/es/ciberseguridad	Diploma			No oficial Híbrido
España	Programa experto en ciberseguridad empresarial	Gestión de la ciberseguridad	EQF5 (CFGS de FP)	Universidad Internacional de Schiller	Privada	https://sibt.schiller.edu/formacion/programa-experto-en-ciberseguridad-empresarial/	Diploma			No oficial Presencial
España	Máster en Redes y Ciberseguridad	Ciberseguridad, seguridad de la información	EQF7 (máster)	CESTE, Escuela Internacional de Negocios	Privada	https://www.ceste.es/programas/mrc-master-en-redes-y-ciberseguridad/	Grado			No oficial 90 ECTS Híbrido
España	Máster Ejecutivo en Gerente de Ciberseguridad	Gestión de la ciberseguridad	EQF7 (máster)	Digital Age University	Privada	https://digitalageuniversity.com/programa/master-in-cybersecurity-manager/	Grado			No oficial
España	Maestría en Ciencias de la Computación - Ciberseguridad, Análisis de Datos e IA	Ciberseguridad, seguridad de la información	EQF7 (máster)	MIA Digital University	Privada	https://miauniversity.com/es/master/master-in-computer-science-cybersecurity-data-analytics-and-artificial-intelligence/	Grado			No oficial en línea
España	Master en Ciberseguridad	Gestión de la ciberseguridad	EQF7 (máster)	Euroinnova International Online Education	Privada	https://www.euroinnova.edu.es/master-ciberseguridad-online	Grado			No oficial 60 ECTS Online

Co-funded by
the European Union

Financiado por la Unión Europea. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente de los autores y no reflejan necesariamente los de la Unión Europea o la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de ellas.