CyberHubs

Cybersecurity Skills Needs Analysis report Spain.

Co-funded by
the European Union

About CyberHubs

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

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

Project consortium

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

Full partners

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

Associated partners

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

Legal Disclaimer

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

Co-funded by the European Union

Copyright © 2024 by CyberHubs

All rights reserved.

Cybersecurity Skills Needs Analysis Spain, 2024, final version.

Deliverable D2.1: "Cybersecurity skills mismatches analysis".

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

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

Revision History			
Version	**Date**	**Modified by**	**Version**
0.1	4/07/2024	Shila Ganguly (UNIR)	Draft version (structure)
0.2	15/07/2024	Gaëlle Candel (AMETIC)	Drafting point 2
0.3	17/07/2024	Alejandro Velasquez (UNIR)	Completion chapters 4 and 5
0.4	29/07/2024	Shila Ganguly (UNIR)	Revision and comments
0.5	20/08/2024	Gaëlle Candel (AMETIC)	Drafting point 3 & 6
0.6	4/09/2024	Alejandro Velasquez (UNIR)	Integrating AMETIC reports. Revision
0.7	16/09/2024	Gaëlle Candel (AMETIC)	Drafting introduction and comments
0.8	19/09/2024	Shila Ganguly (UNIR)	Editing. General revision
0.9	01/10/2024	Marie Montaldo (DIGITALEUROPE)	Review of the document
1.0	05/10/2024	Alejandro Velasquez (UNIR)	Integrating DE suggestions

Table of contents

Executive Summary 7

1 Introduction 9

1.1 Cybersecurity skills in Spain 9

1.2 Research approach 9

1.3 Reading guide 9

2 Desk research (demand) 10

2.1 Data collection 10

2.2 Overview of the national context 12

2.2.1 Politics and agencies 12

2.2.2 Laws and regulations 13

2.2.3 Market 14

2.2.4 Society 14

2.2.5 Technology 15

2.3 Literature 15

2.3.1 Roles 15

2.3.2 Skills 16

2.4 Labour market reports and databases 16

2.4.1 Roles 17

2.4.2 Skills 18

2.5 Conclusions 18

3 Questionnaire 19

3.1 Data collection 19

3.2 Results 19

3.2.1 Cybersecurity roles 19

3.2.2 Skills for cybersecurity professionals 20

3.2.3 Training of cybersecurity professionals 21

3.3 Conclusions 23

4 Job vacancy analysis 24

4.1 Data collection 24

4.2 Results 24

4.3 Conclusions 25

5 Desk research (supply) 26

5.1 Data collection 26
5.2 Results 26
5.3 Conclusions 26
6 Expert panel 27
6.1 Data collection 27
6.2 Results 27
6.2.1 Cybersecurity roles 28
6.2.2 Skills for cybersecurity professionals 28
6.2.3 Training of cybersecurity professionals 29
6.3 Conclusions 30
7 Conclusions 31
7.1 Cybersecurity roles 32
7.2 Skills for cybersecurity professionals 32
7.3 Education and training of cybersecurity professionals 32
8 References 33
9 Annexes 34
9.1 Annex 1: summary of desk research literature (desk research - demand) 34
9.2 Annex 2: cybersecurity training programmes in Spain (desk research - supply) 37

List of Tables

Table 1. Data collection in numbers 12
Table 2: Main results of the job vacancy analysis 24
Table 3: Companies permanently offering cybersecurity job vacancies in Spain 25

List of Figures

Figure 1: Cybersecurity Roles Growth Projection 20
Figure 2: Substantial Skills Needs for Cybersecurity 21
Figure 3: Importance of Cybersecurity Training Strategies 22
Figure 4: Importance of Cybersecurity Qualifications 23
Figure 5: Job Analysis by demand per profiles 24
Figure 6: Classification of Cybersecurity Programs in Spain 26

Executive Summary

Introduction

The Cybersecurity Skills Needs Analysis is the analysis about the current state of art of the cybersecurity in Spain. This report contains the necessary information about all parameters for the Spanish hub, which is one of the key objectives of the project. During the analysis, data about cybersecurity programs in different universities was collected, as well as the documents and references that the country owns for strategic planning in cybersecurity, regulations, and policies in cybersecurity. In addition, the opinion of experts in cybersecurity supported the information collected from private and public companies in Spain through a questionnaire. All this information was correlated with active labour market reports and databases in Spain.

Objective

The Needs Analysis report aims to uncover the critical needs for cybersecurity skills and professional roles in Spain, considering the country's cybersecurity ecosystem status and its opportunities and peculiarities. The goal is to identify and establish ENISA roles in cybersecurity, which currently requires strengthening. These roles refer to specific job profiles and responsibilities in the cybersecurity field, as defined by ENISA (the European Union Agency for Cybersecurity), which are crucial for maintaining and improving Europe's digital security. To achieve this, the focus will be on improving educational programs that address the needs of the labour market and technological capabilities at the national level, it will also feed the development of a country-specific Cybersecurity Skills Strategy with the information on the current and future demand for cybersecurity skills and roles and on the current supply of cybersecurity learning offering. creating a CyberHub, reinforcing the country's cybersecurity.

Approach

This study adopts a multi-method approach whereby both primary and secondary data collection is used as input for the analysis. This approach includes: i) a (demand) desk research to gain insight on potentially relevant cybersecurity roles and skills with a study of the existing literature (scientific papers, labour market reports, and labour market databases) and a job vacancy analysis, ii) a questionnaire to collect data from industry and other relevant actors on the current and future needs for cybersecurity professional roles and skills, iii) a (supply) desk research to get an overview of the current cybersecurity learning offering, and iv) an expert panel to explore future situations and validate the results from the quantitative data collection. This methodological approach uses European frameworks, like the European Cybersecurity Skills Framework (ECSF) and other relevant frameworks, as a foundation to specify the main cybersecurity missions, tasks and skills needed in a professional cybersecurity context, making it a valuable reference for profiling skills and knowledge needed by cybersecurity professionals.

Results

The result of the report shows the aspects that need to be improved in terms of cybersecurity in Spain, identifying the ENISA roles that requires to be strengthened in terms of educational programs, training, capacity building and technological capabilities. Addressing these gaps will create greater opportunities in the labour market for roles that are in high demand, helping to meet the growing need for cybersecurity professionals. The results summarize as follow:

Firstly, within the reports and different analyses consulted and presented in this report, the most required roles for this growing labour market are the following ones:

1. Cybersecurity Implementer.
2. Cybersecurity Architect.
3. Cyber Incident Responder.
4. Cyber Legal, Policy & Compliance Officer.
5. Cybersecurity Risk Manager.

Secondly, and taking in account the questionary, the roles expected to see the highest demand and growth are the following ones:

- Cybersecurity Implementers/Experts
- Chief Information Security Officer (CISO)/Manager (public sector)
- Incident Responders

Evidencing that Spain required more professionals in the following roles by order of importance:

1. Cybersecurity Implementer.
2. Cybersecurity Architect.
3. Cyber Incident Responder.

Conclusions

The most important and in-demand roles in the sector are cybersecurity implementers, cybersecurity architects, and incident responders, who play a crucial role in managing the digital security of organizations.

The roles and needs for professionals are based specially in programming languages, for the implementation, architecture, and analysis of cybersecurity systems. The growing demand for cybersecurity experts with hard skills and the high valuation of critical skills reflect the importance of being prepared for the constantly evolving cyber threats and the modern technologies.

Additionally, there is a significant gap between the supply and demand for cybersecurity professionals in Spain, with the labor market requiring more experts with advanced technical skills. This gap is exacerbated by the "brain drain," as many highly skilled professionals seek opportunities abroad.

1 Introduction

1.1 Cybersecurity skills in Spain

Spain has established itself as a prominent player in the European cybersecurity landscape. The country's National Cybersecurity Strategy, which is continuously updated, reflects a proactive approach to digital security. Despite these efforts, significant challenges remain, particularly the shortage of highly skilled professionals needed to fill critical roles such as cybersecurity implementers, architects, and incident responders. The growing adoption of cloud technologies and artificial intelligence, combined with increasingly sophisticated cyber threats, highlights the need for specialized training in areas like programming and system architecture. Additionally, Spain faces competition from other countries for talent, leading to a "brain drain" of cybersecurity experts. The public sector struggles to keep pace with cybersecurity demands, creating vulnerabilities in the protection of national infrastructure.

1.2 Research approach

The methodology for analyzing country-specific cybersecurity skills needs is common to the seven countries representing the CyberHubs, namely Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain. It uses the well-established European Cybersecurity Skills Framework (ECSF) as a starting point to define skills and knowledge needed in cybersecurity professional roles. This methodology relies on a multi-method approach to collect and analyze both quantitative and qualitative data from multiple sources to identify current and emerging requirements for cybersecurity skills and professional roles. The data collection and analysis focus both on the demand and supply of cybersecurity skills and roles in Spain.

The first step in this study was to identify the current and future demand for cybersecurity roles, competencies, skills, and knowledge by means of a desk research, questionnaire, expert panel, and job vacancy analysis. The second part of the analysis focused on identifying existing learning programs to determine to what extent the current supply of cybersecurity learning programs is sufficient to meet the demand. A gap analysis is then performed, comparing the current and future demand with the existing supply.

Figure 1: Demand and supply data collection and analysis

Overall, this needs analysis provides valuable input for developing national cybersecurity skills strategies. The gap analysis plays a pivotal role in the overall needs assessment, helping to align future demand for cybersecurity roles and skills to the future supply of learning programs for more effective country-specific cybersecurity strategies. .

1.3 Reading guide

This document is organized to first provide a snapshot of Spain's cybersecurity environment, followed by a detailed analysis of the skills required to meet the growing demand for cybersecurity professionals. It concludes with recommendations for addressing the current skills mismatch, focusing on education, training programs, and collaboration between government, academia, and industry to strengthen Spain's cybersecurity ecosystem.

2 Desk research (demand)

2.1 Data collection

In the study, a comprehensive data collection process was conducted to gather insights into the field of cybersecurity, with a specific focus on Spain. The research encompassed a diverse range of sources, including academic literature and labour market reports, to provide a holistic understanding of the subject matter.

Here's a breakdown of the number of items included in the analysis:

Literature Review:

1. Spanish Government, "Digital Spain 2026":
   - Link: https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx.

2. Estrategia Nacional de Ciberseguridad, "A priority, a challenge and a commitment for all". National Strategy of Cybersecurity, by the Spanish Government, 2019. It includes:
   - Threats and challenges in cyberspace.
   - Purpose, principles and objectives for cybersecurity.
   - Executive summary of the national cybersecurity strategy 2019.
   - Link 1: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.
   - Link 2: https://www.aesseguridad.es/news/55/Noticia_03_Estrategia_Nacional_Ciberseguridad.pdf.

3. CCN-CERT, "Approach to Artificial Intelligence and Cybersecurity". Best practice report, October 2023, which includes:
   - Emerging trends.
   - Continuous training.
   - Link: 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, "Standardisation helps prevent cyber-attacks and protect communications, working on aspects ranging from cloud security to electronic evidence management, from IoT (Internet of Things) privacy to security and privacy for Big Data, among others". Article by the Spanish Standardization Association, CTN320 Group on cybersecurity.
   - Link: https://pasosfirmes.es/estandares-seguridad-informatica-ciberataques/.

5. Foro Nacional de Ciberseguridad, "Foro Nacional de Ciberseguridad Motor de la Colaboración Público-Privada - 2023". The National Cybersecurity Forum has published a comprehensive and highly interesting document on the state of cybersecurity in Spain entitled "National Cybersecurity Forum, motor of public-private collaboration - 2023", which includes:
   - Competence framework for higher specialised training programmes in cybersecurity.
   - Report on the needs, capabilities and challenges for public-private collaboration in cyber defence in defence companies.
   - Link: FORO NACIONAL DE CIBERSEGURIDAD. MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA (foronacionalciberseguridad.es).

6. Deloitte, "The state of cybersecurity in Spain - 2023". It includes:
    - Analysis of the state of cybersecurity from the point of view of CISOs and those responsible for cybersecurity in Spain.
    - Link: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html.

7. Disruptive, "Cybersecurity Status Report 2023, Trends, Challenges and Opportunities in Cybersecurity". It includes:
    - Trends.
    - Strategies in Spain.
    - Link: https://ptedisruptive.es/wp-content/uploads/2023/12/Informe-situacion-ciberseguridad-2023_compressed.pdf.

8. Revista Red Seguridad, "Five Things for Cybersecurity Professionals to Be Aware of in 2024". Article by the magazine *Red Seguridad* on the skills of cyber security professionals and future trends.
    - Link: https://www.redseguridad.com/.

Labour Market Desk Research:

9. MordorIntelligence, "Cybersecurity Market in Spain Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)"
    - Link: https://www.mordorintelligence.com/industry-reports/spain-cybersecurity-market.

10. Globaldata, Spain: "Cybersecurity Related Job Trends (October 2023 - January 2024)"
    - Link: https://www.globaldata.com/data-insights/macroeconomic/spain-cybersecurity-related-job-trends-2094774/.

Labour Data Base:

11. Foro Nacional de Ciberseguridad, "Informe Sobre la Cultura de la Ciberseguridad en España". The National Cybersecurity Forum published in 2021 an outstanding report on cybersecurity culture entitled "Report on Cybersecurity Culture in Spain", which includes:
    - Digital Literacy in Cybersecurity.
    - Proposal for actions to be taken in the field of education.
    - Link: https://www.dsn.gob.es/sites/dsn/files/ACCESIBLE%20Trabajos_Foro-Nacional-Ciberseguridad.pdf.

12. INCIBE, "Analysis and Diagnosis of Cybersecurity Talent in Spain - 2022". Study recently published, which includes:
    - Diagnosis of cybersecurity talent in Spain.
    - Definition of a model for characterising cybersecurity profiles in Spain.
    - Link: https://files.incibe.es/incibe/talento/INCIBE_InformeCompleto_DIAG.pdf

13. Fundación Alternativas, "IV Report on Science and Technology in Spain – 2023, Trends, challenges and opportunities in cybersecurity":
    - Link: https://digital.csic.es/bitstream/10261/310469/3/Investigaci%c3%b3n_ciberseguridad_Espa%c3%b1a.pdf.

In total, the study analysed 13 items across literature and labour market reports, providing a comprehensive overview of the current landscape of cybersecurity in Spain, including trends, challenges, and opportunities. This data collection formed the foundation of the research and enabled to draw meaningful conclusions and insights.

Table 1. Data collection in numbers

Data collection in numbers	
Literature	8 papers/ articles included in analysis
Labour market desk research	2 labour market reports
Labour Data Base	3 labour data base reports

Spain, in terms of cybersecurity, is a reference in the European Union. Its strategy is one of the most complete ones and it is constantly updated through various reports and documents, which allow to maintain a real approach of the situation. During the development and collection of reports, documents, and analysis of cybersecurity in Spain, it was evident that there is still a need for more professionals to occupy different job positions that meet the profiles that this project focuses on to increase the national coverage of cybersecurity and cyber defence.

The labour market in Spain is wide and covers different profiles of ENISA. With the labour market desk, it was possible to establish a broad overview of trends and needs in cybersecurity for private and public industry, as well as institutions serving the country.

In these reports and web pages, it was possible to observe in general terms the main needs of the labour market in Spain, but mainly the most representative profiles that currently require more interest from cybersecurity professionals.

2.2 Overview of the national context

Spain has a national cybersecurity strategy, which frames, regulates and performs a prospective analysis in the short, medium and long term of the actions, activities and needs of digital security, where the different private, public and governmental sectors are involved, aligned with internal and international regulations to maintain, manage and fulfil all the needs, requirements and actions regarding cybersecurity.

2.2.1 Politics and agencies

1. Government Actions

   The Spanish government has established the **National Institute for Cybersecurity (INCIBE)** as the lead agency in charge of coordinating cybersecurity policies and strategies at the national level. INCIBE works closely with other government agencies, such as the **National Intelligence Centre (CNI)**, the Ministry of Economic Affairs and Digital Transformation, and the **National Cryptologic Centre (CCN)**, to promote cybersecurity in Spain. The **Guardia Civil and the National Police** have units specialised in cybercrime.

   In addition, the **Centre for Industrial Cybersecurity (CCI)** focuses on the protection of industrial control systems and cybersecurity in the industrial sector.

2. National Strategy and Guidelines

   Spain has a National Cybersecurity Strategy that establishes the lines of action and objectives to protect the country against cyber threats. This strategy covers aspects such as the protection of critical infrastructure, the improvement of public awareness and the promotion of public-private collaboration in cybersecurity matters. The document is: National Cybersecurity Strategy, 2019.

3. Campaigns, Initiatives and Funding Opportunities in Spain

- Día del Internet Seguro: Safe Internet Day is an annual initiative to promote safe online practices among Spanish citizens.
- INCIBE training programmes: cybersecurity training programmes for professionals and student.
- ICT Security Conferences by the CCN.
- Workshop call for funding from the European Digital Agenda: organized in March 2024, investment of 84 million euros.
- Strategic Initiative for Innovative Public Procurement (IECPI): tool promoted by INCIBE in 2021 to foster innovation in cybersecurity from the public sector, specifically through the acquisition of innovative solutions or those in the development phase.
- RETECH Cybersecurity: strategic initiative of the country for the development of the cybersecurity ecosystem (capabilities, industry, R&D, talent, etc.), which, with the coordination of INCIBE, has brought together in its first phase 15 autonomous communities with an initial budget of 149 million euros.
- Global cyber security innovation programme: INCIBE, within the Global Security Innovation Programme, has the particular mission of raising cybersecurity capabilities and resources in the academic, business and technological ecosystems, aimed at boosting the cybersecurity capabilities of society and the economy in general.
- External promotion of industry through ICEX ESPAÑA (a national public business entity whose mission is to promote the internationalisation of Spanish companies and the promotion of foreign investment) and AMETIC.

2.2.2 Laws and regulations

The regulatory landscape in cybersecurity in Spain comprises a combination of national legislation and European Union (EU) regulations. This framework aims to ensure the protection of critical infrastructure, personal data, and digital assets against cyber threats.

In Spain there is a **Code of Cybersecurity Law**, published in the Official State Journal, which cites the main rules to be considered in relation to the protection of cyberspace and ensuring cybersecurity.

In this code, reference is made to the following laws, among others:

- **National Security Scheme** (ENS) - Royal Decree 3/2010.
- **National Security Law**: Organic Law 36/2015, of 28 September, on National Security, which regulates the fundamental principles and bodies, as well as the functions they must perform, for the defence of National Security.
- **Order TIN / 3016/2011**, of 28 October, creating the Commission for Security in Information and Communications Technologies of the Ministry of Labour and Immigration.
- **Law 11/2002**, of 6 May, regulating the National Intelligence Centre.
- Royal Decree 1008/2017, of 1 December, approving the **National Security Strategy 2017**.
- **National Cybersecurity Strategy 2019**.

The following laws cover also the analysed field:

- Organic Law on **Data Protection and Guarantee of Digital Rights** (LOPDGDD): Organic Law 3/2018, of 5th December.
- Law on **Information Society Services and Electronic Commerce** (LSSICE): Law 34/2002, of 11th July.

The implementation of EU legislation, especially in the field of cybersecurity, is supervised by the Spanish authorities in accordance with the principles and directives established by the European Union. Spain transposes EU directives and

regulations into national legislation, ensuring compliance with EU standards and requirements. In addition, Spanish regulators collaborate with EU agencies and participate in EU initiatives and programmes aimed at improving cybersecurity in the Member States.

2.2.3 Market

The cybersecurity market in Spain has a mix of large multinational companies, medium-sized providers and small specialised companies. Key players include:

- **Multinational and big companies**: Symantec Corporation, SIRT, Cisco Systems, Palo Alto Networks, IBM Security and Check Point Software Technologies are some of the multinational companies that have a significant presence in the Spanish market, offering a wide range of cyber security solutions for businesses and consumers.
- **Medium-sized providers**: companies such as Panda Security, Fortinet, Trend Micro, Sophos, GMV, and F-Secure Corporation are prominent in the Spanish cybersecurity market.
- **Small, specialised companies**: it includes ElevenPaths (Telefónica), S21sec, CounterCraft, AlienVault (AT&T Cybersecurity), Vintegris, etc.

The overall value of the cybersecurity market in Spain, which includes software and hardware sales, as well as revenues from the provision of services, reached €1.95 billion in 2022.

The labour market is very wide and changing, it depends a lot on the evolution of information technologies and, on the growth and discovery of new and complex threats in cyberspace. It is evident that there is a worldwide lack of professionals in cybersecurity. Spain is not left behind in this aspect, since being a reference, it is required to be able to meet the needs of industry and institutions to protect the information environment and cyberspace. This is why those with a high level of technological skills are necessary more frequently; the problem lies in the time and dedication required by students to acquire these important knowledge and skills for the work environment in cybersecurity.

2.2.4 Society

Spain is currently a pioneer in the implementation of strategies and plans for innovation in information technologies, training at all academic levels and implementation of new digital information technologies.

- **Digitalisation:** according to the European Commission's DESI (Digital Economy and Society Index) report, Spain has shown steady progress in its digitalisation in recent years. In the DESI 2022 report, Spain ranked 7th out of 27 EU countries in terms of digitisation. The report assesses several indicators, such as connectivity, digitisation of companies and digital skills of the population.
- **Use of digital tools:** according to Spain's National Statistics Institute (INE), in 2023, 95.4% of the population aged 16 to 74 years will have used the Internet in the last three months (0.9 percentage points), 55.9% have shopped on the Internet in the last three months (0.6 points more than in 2022), 66.2% have basic or advanced digital skills. These figures show high internet penetration and widespread use of digital tools among the Spanish population.
- **Cybersecurity awareness**: the Spanish National Cybersecurity Institute (INCIBE) develops cybersecurity awareness and training initiatives aimed at citizens, companies and public administrations.

Spain is a benchmark in cybersecurity in the European Union and the region, and it is currently possible to find nationals playing cybersecurity roles in other countries in the region. In the area of education, it has excellent opportunities to professionalize in aspects and topics related to cybersecurity, as evidenced while conducting the desk research report of official and non-official institutions, and cybersecurity programs.

Companies such as Telefónica and Orange are a clear example of the competitiveness and importance in the information technology sector, maintaining a competitiveness and revenue generated within the top 20 at European level, demonstrating the need for more and better professionals in the field of technology and therefore cybersecurity.

2.2.5 Technology

Digital Spain 2026 is the update of the strategy launched in July 2020 as the country's digital transformation roadmap. Since its presentation, the Recovery Plan for Spain was approved; eight specific plans for its deployment were published; the main investment programmes were launched at national, regional and local level, and decisive progress was made in structural reforms.

The update of the Digital Spain agenda incorporated the priorities for the coming months and two new cross-cutting axes referring to the Strategic Projects for Economic Recovery and Transformation (PERTE) and the RETECH initiative, a network of emblematic strategic transformational projects in the digital area proposed by the autonomous communities.

In this regard, the Spanish government, through the National Cybersecurity Institute (INCIBE), led by the Secretary of State for Digitalisation and Artificial Intelligence, launched the RETECH Cybersecurity initiative. This programme, backed by an initial budget of 149 million euros and the participation of 15 autonomous communities, aims to strengthen the cybersecurity ecosystem in Spain. This initiative is expected to boost research in modern technologies, especially in the field of cybersecurity, and foster technological development in strategic sectors. In addition, the government plans to invest more than €530 million from the Recovery Plan in digitalisation projects, reflecting a clear commitment to technological advancement in the country. Digitalisation is being integrated into various sectors, from e-commerce to public administration and industry, highlighting the wide reach of digital resources in Spanish society.

2.3 Literature

For this study, a search of various dossiers related to training, talent and future trends in the field of cybersecurity was carried out:

- INCIBE, Análisis y Diagnóstico del Talento en Ciberseguridad en España, 2022 (*Analysis and Diagnosis of Cybersecurity Talent in Spain*).
- Deloitte, El estado de la ciberseguridad en España, 2023 (*The status of cybersecurity in Spain*).
- Revista Red Seguridad, Cinco cosas a tener en cuenta por los profesionales de la ciberseguridad durante 2024 (*Five things for cybersecurity professionals to watch out for in 2024*).

2.3.1 Roles

Based on the information gathered, a few jobs in the field of cyber security were identified. The most important ones included:

- Chief Information Security Officer (CISO): this is one of the most crucial roles in an organisation in terms of cybersecurity. The CISO is responsible for leading the information security strategy and ensuring that effective measures are implemented to protect the company's digital assets. We have perceived a lack of CISOs in Spain.
- Cybersecurity architects: with the increased adoption of cloud services, cloud security architects are critical to designing and implementing security solutions that protect data and infrastructure in cloud environments.

- Information security analysts.
- Cyber Incident Responder.
- Network security engineers.
- Cybersecurity Implementer.
- Ethical Hackers: their work is crucial to test the security of an infrastructure and prevent malicious attacks. There is also a lack of ethical hackers in Spain.

In terms of future trends, roles related to artificial intelligence (AI) and cloud security are expected to become increasingly important. With the massive integration of AI into various business areas and the increasing adoption of cloud services, cybersecurity professionals will need to understand the security aspects related to these technologies. In addition, roles related to cyber risk management and data privacy are expected to become more prominent as companies seek to comply with data protection regulations and face new security threats.

2.3.2 Skills

Soft skills play an increasingly important role in the success of cybersecurity professionals. The ability to communicate effectively, both verbally and in writing, is critical for collaborating with other teams and for communicating security findings and recommendations to non-technical stakeholders. In addition, the ability to think critically and solve complex problems is essential to address constantly changing challenges and to develop innovative solutions.

The ability to work in teams, professional ethics and integrity are also key skills for cybersecurity professionals, as they often work in collaborative environments and must make ethical decisions about how to protect information and systems. The ability to adapt quickly to new environments and technologies, as well as to stay up to date on the latest trends and threats in cybersecurity, are also critical skills for success in this highly dynamic field.

Hard skills are the main defence of high-level cybersecurity professionals; these skills from the most technical knowledge allow the implementation and configuration of cybersecurity systems and programs. Their understanding and use are necessary to technically obtain outstanding results in the field of cybersecurity.

The programming of different languages, the knowledge and configuration of networks, incident management, malware analysis and penetration tester, are the technical tools of the acquired knowledge of the cybersecurity man at the service of private and public companies and institutions.

2.4 Labour market reports and databases

The work was based on:

- MordorIntelligence, *Cybersecurity Market in Spain Size & Share Analysis - Growth Trends & Forecasts* (2024 – 2029).
- Globaldata, Spain*: Cybersecurity Related Job Trends*, (October 2023 - January 2024).
- INCIBE, *Analysis and Diagnosis of Cybersecurity Talent in Spain*, (2022).

The cybersecurity market in Spain is experiencing significant growth, with an estimated value of USD 2.27 billion in 2024 and is projected to reach USD 3.21 billion by 2029, representing an annual increase of 7.16%. This growth is due to digitisation in various sectors, which has exposed more entities to cyber-attacks and has led to increased demand for

security services. However, despite this growing demand, there is a shortage of talent in the cybersecurity field, posing additional challenges to meet the market's needs.

The COVID-19 pandemic exacerbated these risks, with more than 150,000 cyber-attacks reported to the Spanish government since its inception. Increasing digitisation and the rise of e-commerce are further driving the need for cybersecurity solutions to protect organisations' data and critical infrastructure.

In this context, the government sector is emerging as a key driver of market growth, as information security and sensitive data are critical to safeguard the operations and integrity of state institutions. Stricter regulations are being implemented to strengthen cyber security measures in the country and ensure the protection of critical infrastructures.

As for the cybersecurity industry in Spain, it is highly consolidated, with strong competition among the main market players. Strategic partnerships are being established to strengthen technological capabilities and offer more innovative solutions to customers as well as to improve cybersecurity service offerings and expand the portfolio of products available in the market.

Despite the consolidation of the cybersecurity industry in Spain, the 2022 INCIBE reported highlights a significant challenge: the shortage of qualified talent. The growing digitalization and increase in cyber threats have generated a high demand for specialized professionals, but the current training does not meet the sector's needs. Although there are educational programs, key competencies such as CEH, OSCP, or CISSP certifications are insufficient. Additionally, the report highlights the low representation of female students (only 18%) and the lack of specialized instructors.

2.4.1 Roles

According to the Analysis and diagnosis of cybersecurity talent in Spain, in 2020, the country had approximately 149,774 professionals in this field, representing 0.26% of the total workforce. However, this figure is insufficient to meet the growing needs of the sector. In 2020, the demand for cybersecurity professionals was estimated to reach 63,191 jobs. This mismatch between supply and demand translates into a shortage of 26,024 professionals that Spain needs to incorporate to address digital security challenges.

Future projections suggest that this situation could persist and even intensify. The exponential increase in cyberattacks, as previously mentioned, with 150,000 daily malware incidents, along with new cybersecurity regulations, is driving even greater demand. Additionally, more than 58% of Spanish companies report difficulties in finding qualified cybersecurity personnel.

Within the reports and different analyses consulted and presented in this report, the most required roles for this growing labour market are the following ones:

1. Cybersecurity Implementer.
2. Cybersecurity Architect.
3. Cyber Incident Responder.
4. Cyber Legal, Policy & Compliance Officer.
5. Cybersecurity Risk Manager.

2.4.2 Skills

As can be seen in the most required roles in the Spanish labour market, hard skills are required. The three main roles most sought after by private companies are cybersecurity implementer, architect, and incident responder. These three roles require high-level knowledge and preparation in cybersecurity and technological systems.

- Networking and System Administration.
- Security Incident Handling and Response.
- Understanding of Operating Systems.
- Network Security Control.
- Malware Prevention and Detection.
- Mastery in Coding and Encryption.
- Implementation and Management of Cloud Systems.

2.5 Conclusions

The main barrier to the growth of the cybersecurity sector in Spain is the shortage of qualified talent. In the short term, this deficit will remain a challenge for the sector, driven by the growing digitisation and the increase in cyberattacks. Although companies are facing difficulties in filling the necessary positions, the adoption of strategic partnerships and intensive training programs could partially alleviate this pressure in the coming years. Additionally, the implementation of new cybersecurity regulations will continue to drive the need for specialised professionals.

In the long term, technological evolution and regulatory changes will continue to drive increasing demand for cybersecurity talent, which will require ongoing investments in training and the development of specialised skills. Both the government and companies will need to collaborate on designing education and continuous training strategies, as well as creating incentives to attract and retain qualified talent in this field. This will be crucial to address future challenges in an environment of increasingly sophisticated cyber threats.

The most important and in-demand roles in the sector are cybersecurity implementers, cybersecurity architects, and incident responders, who play a crucial role in managing the digital security of organisations. Also essential are risk managers and compliance experts, roles that are gaining importance due to the increasing number of cybersecurity regulations and policies that companies must comply with.

3 Questionnaire

3.1 Data collection

The questionnaire was distributed via email to more than 100 organizations, covering various sectors such as information and communication, professional, scientific, and technical activities, and public administration. It was also published on AMETIC's LinkedIn page, which has more than 14,000 followers, and on UNIR iTED LinkedIn page, with more than 600 followers, achieving significant visibility online. Additionally, it was shared on AMETIC's X account and UNIR iTED X account to increase its reach. The questionnaire was answered by numerous organizations, large and medium-sized companies, reflecting their greater capacity and need to implement robust cybersecurity measures. The responses covered categories such as the sector of the organization, size, and existing cybersecurity structure.

3.2 Results

In the current context, cybersecurity has become fundamentally important for organizations, regardless of their size or sector. The survey conducted by the Spanish CyberHub provided a detailed view of how companies were addressing this growing need, focusing on three key areas: cybersecurity roles, skills, and training. This analysis not only revealed current trends but also future projections regarding demands and strategies in the field of cybersecurity.

3.2.1 Cybersecurity roles

According to the surveyed companies, the roles expected to see the highest demand and growth are the following ones:

- **Cybersecurity Implementers/Experts:** this is the role with the most significant growth projection. Currently, 90.91% of companies already have a cybersecurity implementer or expert, and demand for these professionals is expected to grow by 38.56% over the next two years. In the long term, this demand could increase dramatically by 111.69%, reflecting the growing need for experts who can implement and manage the necessary security solutions to protect organizations against cyber threats.
- **Chief Information Security Officer (CISO)/Manager:** with 77.27% of companies already having a CISO or information security manager, this role also shows expected growth, although more moderate. A 25% increase in demand for this position is anticipated over the next two years, and a 60% increase in the long term. This underscores the importance of strong and strategic leadership in cybersecurity that can direct and oversee the organization's security policies.
- **Incident Responders:** although 63.64% of companies currently have an Incident Responder, the demand for these professionals is significant, with a projected growth of 56.25% over the next two years. In the long term, demand for Incident Responders is expected to increase by 112.5%, highlighting the critical need to be prepared to respond quickly and effectively to any security incidents that occur.

The following chart illustrates the projected growth in demand for key cybersecurity roles according to the surveyed companies.

Figure 1: Cybersecurity Roles Growth Projection

3.2.2 Skills for cybersecurity professionals

In the realm of cybersecurity, it is crucial not only to have specific roles within organizations but also to have a set of technical and strategic skills that allow them to face various cyber threats. The survey identified the most valued and demanded skills by companies in this field. These skills reflect not only the current need but also the areas in which organizations are investing to secure their infrastructure and data.

As shown in the following chart, the most in-demand skills include:

- **Data Privacy and Data Security and Cryptography:** both skills are of "substantial need" by 56% of the organizations surveyed. This underscores the importance of protecting sensitive information and ensuring data security through cryptographic methods.
- **Cloud Security and Access Control/Identity Management:** 48% of organizations identified these skills as having a "substantial need." With the growing adoption of cloud solutions, these competencies are essential for ensuring secure and controlled access to digital resources.
- **Systems and Network Security:** like data privacy skills, systems and network security are also seen as having a "substantial need" by 56% of organizations. This skill is crucial for protecting critical infrastructure against cyberattacks.
- **Supply Chain Security:** with 48% identifying it as a "substantial need," this skill reflects the growing concern for ensuring that all links in the supply chain are resilient to cyber threats.

These areas reflect a high awareness and need for strengthening critical cybersecurity capabilities.

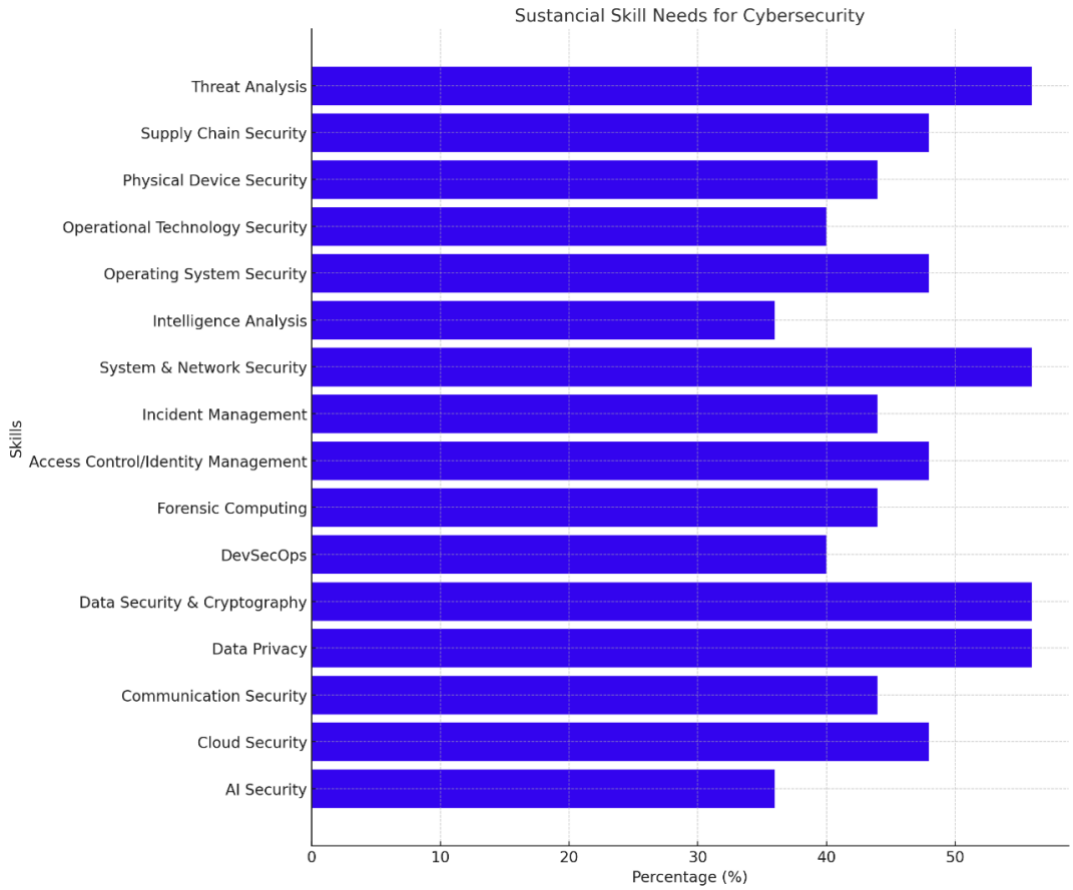

Figure 2: Substantial Skills Needs for Cybersecurity

3.2.3 Training of cybersecurity professionals

Importance of the Cybersecurity training strategies:

84% of organizations indicated a high need for training, primarily due to technological developments and changes in organizational infrastructure. However, 40% faced delays in training, which could compromise their preparedness against cyber threats. The most valued training strategies included:

- **Hiring and training people:** 69.57% considered it "very important."
- **On-the-job training and coaching:** also 69.57% considered it "very important."
- **External training:** 52.17% considered it "very important."

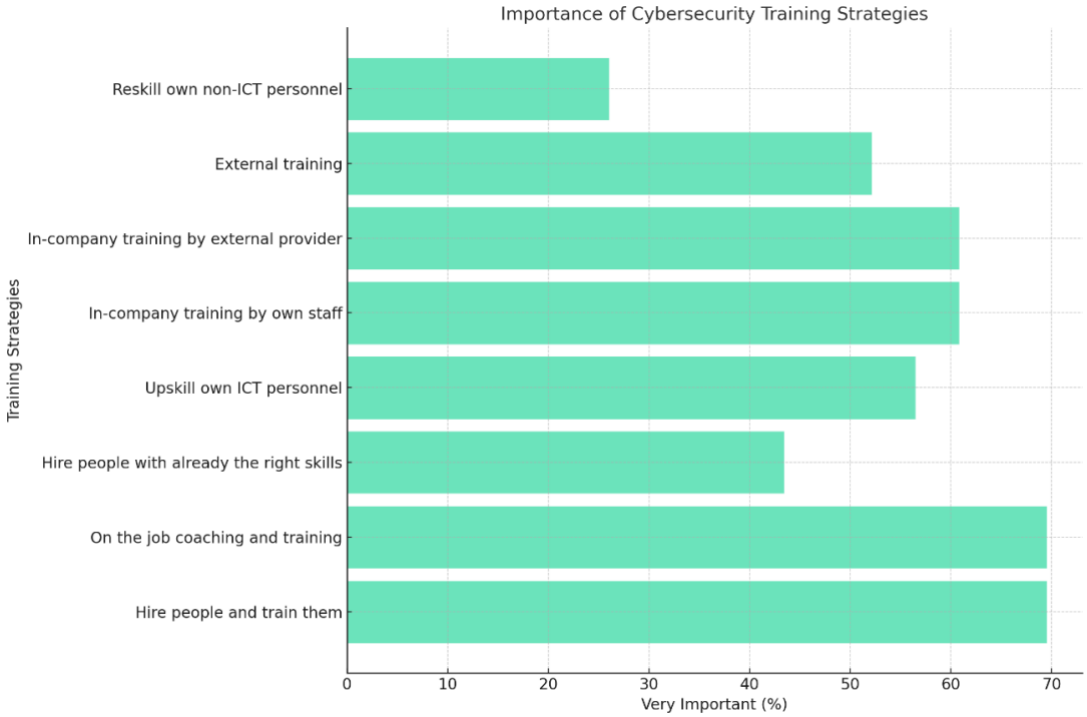

Figure 3: Importance of Cybersecurity Training Strategies

Importance of Cybersecurity qualifications:

A significant portion of organizations emphasized the critical need for formal qualifications when hiring cybersecurity personnel. According to the data, organizations are prioritizing specific certifications and educational backgrounds to ensure preparedness against cyber threats.

- **Formal certification relevant for the role:** 69.57% of organizations rated this as "very important."
- **Bachelor/master's degree relevant for the role:** another 69.57% also considered this "very important."
- **Formal professional education relevant for the role:** 56.52% of organizations saw this qualification as "very important."
- **Certificates for participation in courses:** 47.83% rated these as "very important."

This data highlights the importance of formal and certified education in addressing cybersecurity challenges, helping organizations build a robust defense against evolving threats.

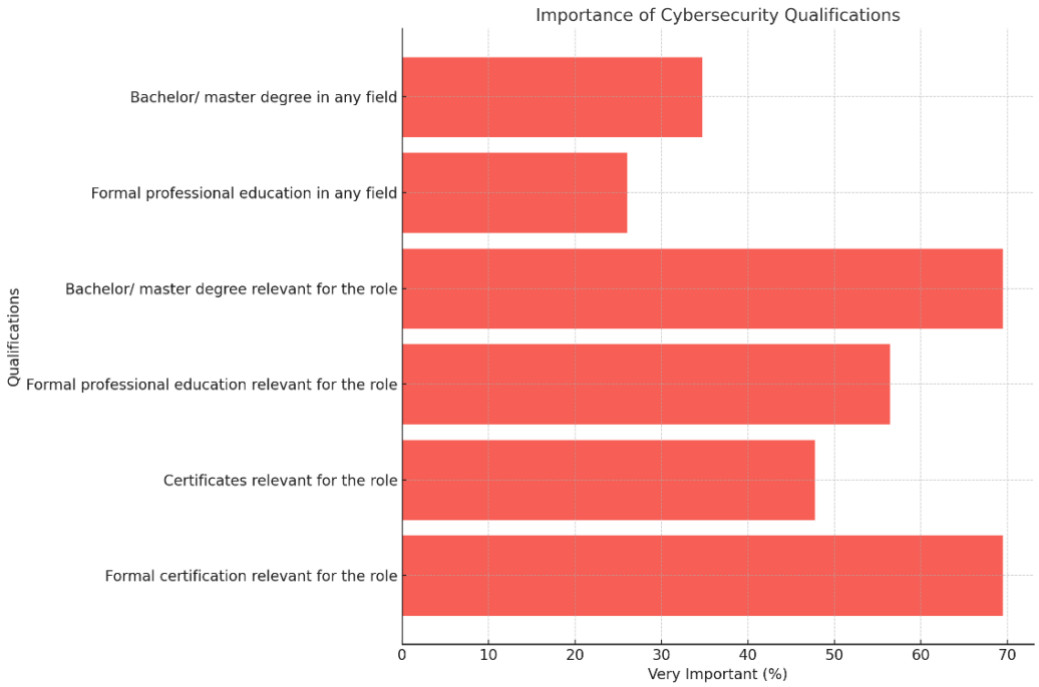

Figure 4: Importance of Cybersecurity Qualifications

3.3 Conclusions

In conclusion, the questionary highlighted the urgent need for specialized roles, advanced technical skills, and continuous training to address the cybersecurity challenges in today's business environment.

The roles and needs for professionals are based specially in programming languages, for the implementation, architecture, and analysis of cybersecurity systems.

The growing demand for cybersecurity experts with hard skills and the high valuation of critical skills reflect the importance of being prepared for the constantly evolving cyber threats and the modern technologies.

Moreover, although companies are advancing in their cybersecurity strategies, delays in training represent a significant risk that must be addressed urgently. A more robust strategic planning in training and skill development will be crucial to maintaining long-term competitiveness and security.

4 Job vacancy analysis

4.1 Data collection

The information obtained for the job vacancy analysis was extracted from the following sources:

- **Glassdoor:** search engine for job and work experience. Link: https://www.glassdoor.com/about/.
- **Indeed:** job search. Link: https://www.indeed.com/.
- **LinkedIn:** social network oriented to business use, business and employment. Link: https://www.linkedin.com/.
- **Infosec Jobs**: job search. Link: https://infosec-jobs.com/.
- **Himalayas:** application for job search from home. Link: https://himalayas.app/jobs.

4.2 Results

Table 2: Main results of the job vacancy analysis

Job Titles (ESCF Matched):	Job Titles (ESCF Matched) #:	Skill Category:	Skill Category #:
Cybersecurity Implementer	469	Cybersecurity (Hard skills)	5333
Cybersecurity Architect	159	IT (Profession Related Skill)	3449
Cyber Incident Responder	124	Transversal (soft) Skills	3145
Cyber Legal, Policy & Compliance Officer	81	Organisational Skills	1648

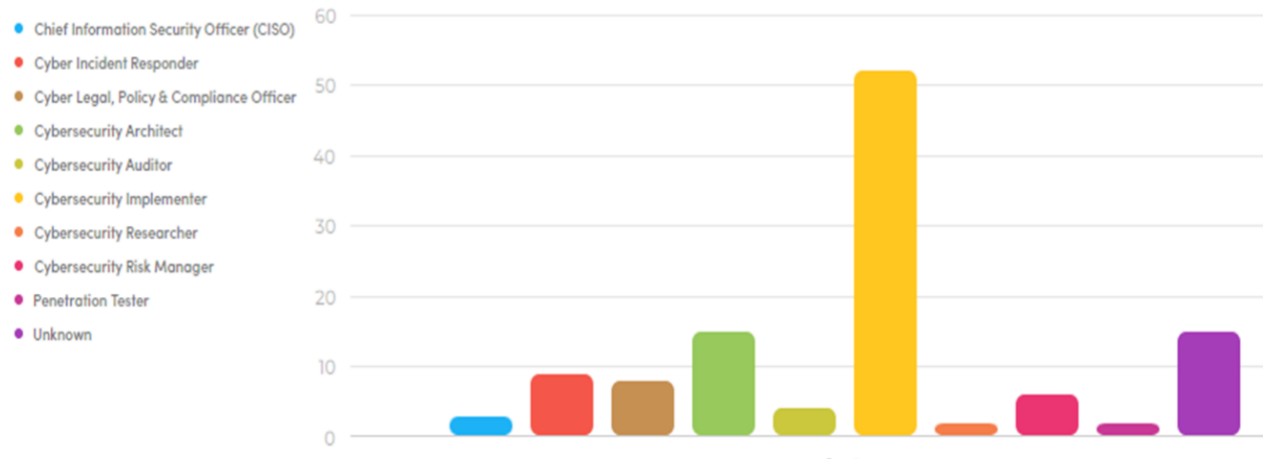

Figure 5: Job Analysis by demand per profiles

The results provided by the search engines used during the search for vacancies in Spain for cybersecurity positions specifically for the different roles of ENISA, showed 5 main companies that are permanently offering job vacancies:

These 5 companies are:

Table 3: Companies permanently offering cybersecurity job vacancies in Spain

EY	Provides audit, tax, transaction advisory, and consulting services
Capgemini	Provides IT and consulting services, outsourcing and professional services
Palo Alto Networks	U.S. multinational cybersecurity company
Deloitte	Provides audit, consulting, financial advisory, risk advisory, tax, tax, legal, and advisory services
Grupo Santander	A Spanish multinational financial company

4.3 Conclusions

The results provided by the information gathered allow to see that Spain requires cybersecurity professionals in the roles where hard skills are most needed, mainly where knowledge in programming, network administration and configuration, network architecture and cybersecurity systems, are the basis for strengthening security levels in companies and institutions.

This is why there is an evident need for more professionals in the roles of Cybersecurity Implementer, Cybersecurity Architect and Cyber Incident Responder, as these positions require greater depth in the knowledge of information technology and computer systems. In addition, the handling of programming languages and data networks such as architecture and implementation are the pillars of the previous preparation at the time of applying for these positions.

In Spain, unlike other countries participating in the project, the role of Chief Information Security Officer (CISO) has been strengthened.

Integrating the information obtained on the labour market, it is evidenced that effectively at national level roles such as CISO and Ethical hackers, are being covered at private level outstandingly and public at a lower level, since, although there are requests and requirements netin these fields, it is affordable for the market to find professionals to cover them.

In contrast to the above, there is an evident need for professionals in roles where hard skills are required, such as cybersecurity implementers, cybersecurity threat analysts and architects for cybersecurity systems, which shows that it is necessary to obtain a greater number of professionals with programming experience.

5 Desk research (supply)

5.1 Data collection

The information collected on cybersecurity programs in Spain was divided into official and unofficial ones. The sample of the main programs with a high level of evaluation of both the program and the institution was collected. In addition, the topics taught within the programs were analysed and verified, as well as the number of hours and credits for each subject.

Finally, their alignment with the ENISA roles, the basis of this project, was considered.

From the point of view of ENISA roles, these programs were focused on roles such as CISO, Cybersecurity Risk Manager and Penetration Tester, the latter with a previous knowledge of hard skills at the time of applying to the program.

The unofficial programs included in this report were focused on the acquisition of more specific skills from the technical level, such as ethical hacking and cyber threat intelligence.

5.2 Results

A total of 43 programs were taken, out of which 30 were official and 13 unofficial. From these 30 official programs, 21 were masters and 9 were bachelor's programs, focused on cybersecurity. Most of them were online or face-to-face in a mixed version. These official programs were offered by the main universities in Spain. Their programs were general and seek to cover various profiles of interest within the cybersecurity environment.

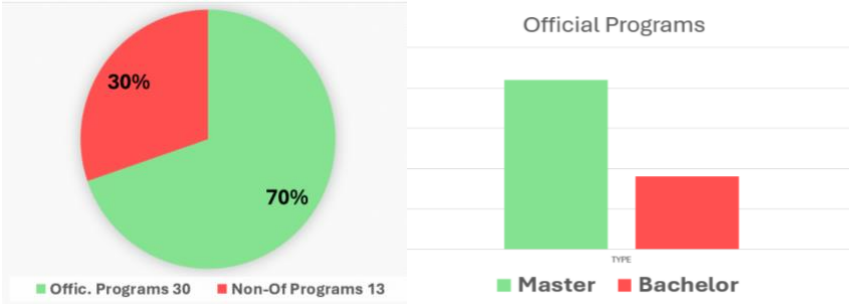

Figure 6: Classification of Cybersecurity Programs in Spain

5.3 Conclusions

From the point of view of ENISA roles, the 30 official programs considering their contents are focused on roles such as CISO, Cybersecurity Risk Manager and Penetration Tester, the latter requiring a previous knowledge of hard skills at the time of applying to the program.

The unofficial programs included in this report are focused on the acquisition of more specific skills from the technical level, such as ethical hacking and cyber threat intelligence.

Having carried out this analysis, and once the contents of the most relevant programs at the national level have been verified, it can be concluded that training and education in the field of cybersecurity at the national level requires an effort to strengthen the roles of high-level capabilities in implementation, architecture and analysis of cybersecurity systems, thus strengthening training in programming languages and design of new technologies and systems for cybersecurity.

6 Expert panel

6.1 Data collection

The cybersecurity expert panel organized within the framework of the Cyber Hub project took place on July 18th, 2024, and featured the participation of prominent professionals in the field. The panel's objective was to explore the current state and future prospects of cybersecurity, with a particular focus on the roles, skills, and training needed to strengthen this field.

The panel was composed of the following experts:

- 1 Marketing and Communications Director from a cybersecurity provider.
- 1 Telecommunications Engineer & Cybersecurity Expert from a non-profit research and innovation center.
- 1 Chief Operating Officer from a consultancy firm specialized in digital transformation and process optimization.
- 1 CEO & Cybersecurity Expert from a cybersecurity company.
- 1 Industrial Engineer & President from a non-profit organization focused on promoting and increasing the women participation in the field of cybersecurity.
- 1 CIO/CTO from a non-profit association that promotes the development of a blockchain ecosystem.
- 1 Computer Engineer, Cybersecurity Expert, from a high education institution.
- 1 Director from a non-profit business association that represents the technology and digital industry.

The meeting lasted two hours and was held virtually, allowing for dynamic and accessible participation from all experts.

With the aim of comprehensively addressing the current challenges and needs in the field of cybersecurity, the panel was structured into two discussion tables:

1. **Industry Table:** focused on exploring the specific needs and challenges that companies face in terms of cybersecurity, including the demand for professionals, required competencies, and interaction with the educational sector.

2. **Ecosystem Table:** centered on analysing the importance of awareness and cybersecurity culture at the societal level, as well as collaboration among various actors to foster a safer and more resilient digital environment.

This division allowed for a more focused and in-depth discussion in each area, facilitating the identification of specific problems and solutions from complementary perspectives.

The panel addressed three central themes in both tables:

- Roles in cybersecurity.
- Skills needed for cybersecurity professionals.
- Training of these professionals.

Below, the qualitative results of the discussions are explained, accompanied by quotes reflecting the consensus among the participants.

6.2 Results

1. **Lack of experts:** there is a significant shortage of professionals with specific skills in development engineering, industrial engineering, and programming. This shortage has led many companies to seek foreign talent to meet these critical needs. As the CEO & Cybersecurity Expert of a cybersecurity company highlighted:

"There is a clear lack of experts in development engineering. We often have to rely on engineers from other countries to meet these critical needs."

Additionally, the Cybersecurity Expert of the university expressed:

"There is a shortage of implementers, cybersecurity architects, and incident response experts."

2. **Need for specific training:** the importance of strengthening training in critical areas such as programming and system implementation is emphasized. This lack of specialized training limits organizations' ability to develop and maintain robust security infrastructures. Moreover, the Chief Operating Officer of the consultancy added:

"It is crucial that the training of professionals includes not only technical skills but also a clear understanding of cybersecurity regulations, something that many CISOs do not yet fully master."

3. **Challenges in the public sector:** public administrations, especially smaller ones, face serious challenges in complying with security regulations due to a lack of resources and knowledge. This creates significant vulnerabilities in the protection of public data and services. The Chief Operating Officer of the consultancy expressed this concern:

"Small administrations lack the resources and knowledge needed to comply with security regulations, leaving them exposed to vulnerabilities." He also added, "In terms of structure, governance, and roadmap, there is still much to be done."

6.2.1 Cybersecurity roles

Professionals with high-level cybersecurity skills are required as the evolution and constant growth of technologies and therefore of cyber threats, requires greater preparation and knowledge in cybersecurity.

In fact, more professionals are needed in the following roles by order of importance:

1. Cybersecurity Implementer.

2. Cybersecurity Architect.

3. Cyber Incident Responder.

6.2.2 Skills for cybersecurity professionals

Strengthening cybersecurity structure:

1. **Regulatory framework:** the creation of a Spanish cybersecurity agency was proposed to standardize and normalize guidelines to facilitate the implementation of cybersecurity policies. A robust regulatory framework is essential to ensure that cybersecurity practices are implemented consistently across the country. The Chief Operating Officer of the consultancy suggested:

"Promote a regulatory framework and create an oversight authority to standardize and normalize guidelines."

2. **Public-Private collaboration:** collaboration between public administration and the private sector is seen as fundamental to improving the implementation of cybersecurity measures. This cooperation is crucial for sharing knowledge, resources, and best practices. The cybersecurity expert of the university emphasized:

"A stronger integration between the state, education, and the private sector is necessary to create a society prepared for this digital era."

3. **Dynamism and adaptation:** the rapid technological evolution requires agile and flexible regulation. Additionally, greater integration between universities and companies is needed to ensure that cybersecurity training and practices evolve alongside market needs. The CEO & Cybersecurity Expert of a cybersecurity company commented:

"Dynamism in regulation and constant adaptation to technological changes is important."

6.2.3 Training of cybersecurity professionals

Roles of the educational sector:

1. **Facilitating entry into the job market:** it is essential that vocational training programs (VET) include internships that allow students to gain experience in real work environments. These internships are crucial for new professionals to develop the skills needed to face current cybersecurity challenges. The Cybersecurity Expert, from a non-profit research and innovation center highlighted:

"Students graduating from vocational and university programs need more opportunities to apply what they've learned. It's crucial they have access to internships to develop these skills."

2. **University-Industry collaboration:** the importance of high education institutions getting closer to companies to adapt academic training to the practical needs of the labour market was emphasized. This collaboration would ensure that students are better prepared to meet the specific demands of the cybersecurity sector. The CEO & Cybersecurity Expert of a cybersecurity company emphasized:

"High education institutions need to get closer to companies. Cybersecurity is a very closed field, where companies are reluctant to share their knowledge. This makes it difficult for new professionals to gain the practical experience that is so needed."

3. **Interdisciplinary programs:** the creation of degrees that integrate disciplines such as law and artificial intelligence is seen as a necessary trend. These programs require close collaboration between industry and academia to develop a curriculum that combines technical knowledge with an understanding of legal and ethical implications. The Chief Operating Officer of a consultancy mentioned:

"Degrees that combine various disciplines, such as legal and AI, are being created. Industry and academia need to work closely together."

Ecosystem Table: Evangelization and Awareness in Cybersecurity Awareness and Cyber Culture:

1. **Cybersecurity Evangelization:** the need to promote a cybersecurity culture at all levels, not only in the business realm but also at the societal level, was highlighted. Education and awareness in cybersecurity are essential for all actors to understand and assume their responsibilities. The CIO/ CTO, of a non-profit association noted:

"It's vital to evangelize about cybersecurity and raise awareness in companies about the importance of implementing a cyber culture at all levels."

2. **Shared Responsibility:** cybersecurity is a collective responsibility. It is crucial to convey this message to create broad awareness of cybersecurity risks and best practices, both professionally and personally.

3. **Diversity:** a critical issue that was not addressed in the survey is diversity within the sector. The lack of diversity represents an area for improvement in future projects, as a more inclusive approach could enhance innovation and effectiveness in cybersecurity strategies. The industrial engineer, President & Founder of a non-profit organization criticized:

"Diversity was not addressed in the survey, which is an area we must tackle in future projects."

6.3 Conclusions

1. **Shortage of Qualified Professionals:** there is still a shortage of qualified professionals, and it is crucial to close the training loop with greater job placement. The Cybersecurity Expert, of a non-profit research and innovation center concluded:

"We must facilitate the entry of young professionals into the job market through internships, so they don't end up without a job after their training."

2. **State-Education-Private Sector Integration:** it is vital that these three pillars work together to prepare society for the challenges of cyberspace. Collaboration and alignment of objectives between these sectors are essential to creating a safe and resilient environment in the digital age.

3. **SWOT Analysis of the Sector:** it is suggested to conduct a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to address cybersecurity challenges at all levels of society. This analysis would allow identifying priority areas and designing effective strategies to strengthen cybersecurity.

7 Conclusions

By integrating and correlating all the information collected during the development of the project, it has been possible to highlight the strengths, weaknesses, opportunities, and threats that cybersecurity currently has in Spain.

Strengths:

The national cybersecurity strategy is aligned with regulation, innovation, and implementation of current and new technologies. This includes all levels of society and national institutions, such as the private sector.

Education and training in cybersecurity is wide and varied and it is possible to obtain it online or in person. University and specialization programs have a prominent level for the acquisition of knowledge in cybersecurity, and there are plans and scholarships that allow applicants to achieve their degrees more easily.

Private enterprise has good technological capabilities for cybersecurity, as well as the defence sector has a high level of cyber defence capabilities.

The implementation and innovation in new and future information technologies is at a proficient level, allowing the generation of new positions and jobs and maintaining a constant flow of job applications for cybersecurity professionals.

Weaknesses:

The lack of cybersecurity professionals, especially those who have knowledge of the skills and capabilities to occupy positions where hard skills are required. This is aligned with the fact that educational programs are not focused on teaching specific high-level cybersecurity topics.

Although the salaries and remuneration of cybersecurity professionals in Spain is good, it is evidenced that it is lower than in other countries, which generates a flight of cybersecurity professionals to other countries in the region.

The public sector is weakest part of the chain, and, although it has elements that support it, it is the area where cybersecurity professionals and implementation of systems and technologies are most needed.

Opportunities:

Education and training in cybersecurity are innovating and advancing in a very good way at national level, which allows to maintain and obtain better professionals and to have a better knowledge of the needs in the digital environment and therefore in cybersecurity.

The private enterprise at the national level has taken important steps in the innovation of cybersecurity, as there are large companies and entities with excellent technological capabilities that can serve the other components of the national environment**.**

Threats:

The constant innovation and advancement of cybercrime, as well as all those groups or potential threats that are growing and can take advantage of the weaknesses described above.

The flight of professionals to other countries in the region with excellent knowledge in cybersecurity.

7.1 Cybersecurity roles

Although professionals are needed at the national level in all roles, this study has allowed to show that an increase in the number of professionals in the following roles is required:

1. Cybersecurity Implementer.

2. Cybersecurity Architect.

3. Cyber Incident Responder.

Professionals with knowledge in programming languages and hard skills are required for the implementation and architecture of cybersecurity systems.

The profiles as CISO, Ethical Hacking, cyber threat intelligence are covered in satisfactory level, mainly the CISO profile.

The public sector in Spain needs an improvement in all the profiles related to cybersecurity technologies.

Lastly, the shortage of experts in these areas leads companies to seek talent abroad.

7.2 Skills for cybersecurity professionals

Cybersecurity education and programs in official and non-official educational institutions require a special focus, strengthening the learning of hard skills, mainly in programming languages for cybersecurity.

The implementation of cybersecurity, architecture and incident responding are the specific requirements for the cybersecurity programs, focusing on hard skills.

It is necessary to strengthen the public sector with more CISO and Cyber Theat intelligence professionals, as this is the strong field in Spain.

As a robust regulator framework was suggested in the expert panel, a specific knowledge and handling of law and public policies is needed. This knowledge could be considered as new skills for professionals in cybersecurity.

7.3 Education and training of cybersecurity professionals

Programs focused on the following fields of cybersecurity education are required:

- Programming languages for cybersecurity.
- Implementation of cybersecurity systems.
- Cybersecurity systems architecture.

It is required to strengthen the programs that already exist and to introduce new ones, focusing in areas like programing for cybersecurity, development of cybersecurity systems and innovative technologies for defense, response and reversing. These training programs should facilitate to recent graduates the entry to labour market. There is also a need of adapting or creating training programs to a more interdisciplinary one.

Lastly, high education institutions and training institutions must work more closely with the private sector to ensure that students are better prepared to meet industry demands.

8 References

- CCN-CERT. (2023). *Approach to Artificial Intelligence and Cybersecurity: Best practice report.*
- Deloitte. (2023). *The state of cybersecurity in Spain.*
- Disruptive. (2023). *Cybersecurity Status Report 2023: Trends, Challenges and Opportunities.*
- ENISA (2022) European Cybersecurity Skills Framework Role Profiles — 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 Report on Science and Technology in Spain: Trends, challenges and opportunities in cybersecurity.*
- GlobalData. (2023). *Spain: Cybersecurity Related Job Trends (October 2023 - January 2024).*
- INCIBE. (2022). *Analysis and Diagnosis of Cybersecurity Talent in Spain*. Instituto Nacional de Ciberseguridad.
- Mordor Intelligence. (2024). *Cybersecurity Market in Spain Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029).*
- Revista Red Seguridad. (2023). *Five Things for Cybersecurity Professionals to Be Aware of in 2024.*
- Spanish Government. (2022). *Digital Spain 2026*. Ministerio de Asuntos Económicos y Transformación Digital.
- Spanish Government. (2019). *Estrategia Nacional de Ciberseguridad: A priority, a challenge and a commitment for all.*
- UNE. (n.d.). *Standardisation helps prevent cyber-attacks and protect communications.* Asociación Española de Normalización.

9 Annexes

9.1 Annex 1: summary of desk research literature (desk research - demand)

Name	Published in	Authors	Year	Language	Link	Key topic(s)	Abstract
Estrategia Nacional de Ciberseguridad	PCI/487/2019, de 26 de abril	Departamento de Seguridad Nacional	2019	Spanish	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.
National Cybersecurity Strategy	PCI/487/2019, april 26	National Security Department	2019	English	https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019	Threats and challenges of cyberspace. Purpose, principles and objectives for cybersecurity.	The National Cybersecurity Strategy defines objectives, sets out the principles, identifies the different current and potential threats in cyberspace and provides clarity on the articulation of efforts between individuals, civil society, private and public organizations in cybersecurity matters; it also defines the governance model for the implementation, monitoring and evaluation of Spain's national cybersecurity.
Estrategia Nacional de Ciberseguridad. España 2019 Una prioridad, un reto y un compromiso para todos.	26 de abril 2023	Manuel Sánchez Gómez-Merelo	2023	Spanish	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.

Name	Published in	Authors	Year	Language	Link	Key topic(s)	Abstract
Análisis y Diagnóstico del Talento en Ciberseguridad en España	mar-22	INCIBE	2022	Spanish	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	Spanish	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	Spanish	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, tomaron muestra de empresas privadas y sus experiencias en ciberseguridad a nivel nacional.
CIBERSEGURIDAD Informe de situación 2023	2023	Disruptive.	2023	Spanish	https://ptedisruptive.es/wp-content/uploads/2023/12/Informe-situacion-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	Spanish	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 reporte 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.

Name	Published in	Authors	Year	Language	Link	Key topic(s)	Abstract
APROXIMACIÓN A LA INTELIGENCIA ARTIFICAL Y LA CIBERSEGURIDAD	oct-23	CCN-CERT	2023	Spanish	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	Spanish	https://www.redseguridad.com/	Tendencias futuras	Artículo en relación a las competencias de los profesionales de la ciberseguridad y las tendencias futuras

9.2 Annex 2: cybersecurity training programmes in Spain (desk research - supply)

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete program me (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	Máster Universitario en Ciberseguridad	Cybersecurity defensive	EQF7 (master)	Universidad de Alcalá	Public	https://www.uah.es/es/estudios/Ciberseguridad/	Degree	47	20	Official, 60 ECTS complete y 30 ECTS parcial
Spain	Máster Universitario Online en Ciberseguridad	Cybersecurity management	EQF7 (master)	Universidad Alfonso X El Sabio	Private	https://www.uax.com/titulaciones/master-en-ciberseguridad-online	Degree	10	40	Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad	Cybersecurity, information security	EQF7 (master)	Universidad de Alicante	Public	https://web.ua.es/es/masteres/ciberseguridad/master-universitario-en-ciberseguridad.html	Degree	147	20	Official 60 ECTS semi campus and online
Spain	Máster Universitario en Seguridad Informática (Ciberseguridad)	Information security	EQF7 (master)	Universidad de Cádiz	Public	https://esingenieria.uca.es/docencia/masteres/master-en-ciberseguridad-datos-informacion/	Degree	10	30	Official 60 ECTS campus
Spain	Máster Universitario en Ciberseguridad	Cybersecurity defensive	EQF7 (master)	Universidad Camilo José Cela	Private	https://www.ucjc.edu/master/ciberseguridad/	Degree	147	50	Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad	Cybersecurity Analyst	EQF7 (master)	Universidad Carlos III de Madrid	Public	https://www.uc3m.es/master/ciberseguridad	Degree	96	60	Official 60 ECTS campus
Spain	Graduado o Graduada en Ciberseguridad	Information security and cybersecurity	EQF6 (bachelor)	Universidad Euneiz	Private	https://www.euneiz.com/grados-universitarios/grado-ciberseguridad/	Degree	156	40	Official 240 ECTS campus

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete programme (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	Graduado o Graduada en Ingeniería de la Ciberseguridad	Information security and cybersecurity	EQF6 (bachelor)	Universidad Europea de Madrid	Private	https://universidadeuropea.com/grado-ciberseguridad-madrid/	Degree	18		Official 240 ECTS campus
Spain	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones	Cybersecurity management	EQF7 (master)	Universidad Europea de Madrid	Private	https://universidadeuropea.com/master-ciberseguridad-madrid/	Degree	10	35	Official 60 ECTS campus
Spain	Graduado o Graduada en Gestión de la Ciberseguridad	Ethical Haking	EQF6 (bachelor)	Universidad Francisco de Vitoria	Private	https://www.ufv.es/estudiar-grado-gestion-ciberseguridad-madrid/	Degree	6	60	Official 240 ECTS campus
Spain	Graduado o Graduada en Ciberseguridad	Information security and cybersecurity	EQF6 (bachelor)	Internacional de La Rioja	Private	https://www.unir.net/ingenieria/grado-ciberseguridad/	Degree	99	1200	Official 240 ECTS campus and online
Spain	Máster Universitario en Ciberseguridad	Information security and cybersecurity	EQF7 (master)	Internacional de La Rioja	Private	https://www.unir.net/ingenieria/master-seguridad-informatica/	Degree	8	750	Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad	Information security	EQF7 (master)	Internacional Isabel I de Castilla	Private	https://www.ui1.es/oferta-academica/master-en-ciberseguridad	Degree	47		Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad	Cybersecurity management	EQF7 (master)	Universitat Internacional Valenciana	Private	https://www.upv.es/titulaciones/MUCC/	Degree	19	30	Official 90 ECTS semi campus and online
Spain	Máster Universitario en Seguridad Informática	Information security	EQF7 (master)	Universidad de Jaén	Public	https://www.ujaen.es/estudios/oferta-academica/masteres/master-universitario-en-seguridad-informatica	Degree	47	30	Official 60 ECTS semi campus and online

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete program me (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	Máster Universitario en Ciberseguridad e Inteligencia de Datos	Cybersecurity management	EQF7 (master)	Universidad de La Laguna	Public	https://www.ull.es/masteres/ciberseguridad-inteligencia-datos/	Degree	19	30	Official 60 ECTS semi campus and online
Spain	Máster Universitario en Investigación en Ciberseguridad	Digital forencics	EQF7 (master)	Universidad de León	Public	https://www.unileon.es/estudiantes/oferta-academica/masteres/mu-investigacion-ciberseguridad-online	Degree	3	60	Official 60 ECTS online
Spain	Graduado o Graduada en Ciberseguridad e Inteligencia Artificial	Information security and cybersecurity	EQF6 (bachelor)	Universidad de Málaga	Public	https://www.uma.es/grado-en-ciberseguridad-e-inteligencia-artificial/	Degree	21	65	Official 240 ECTS campus
Spain	Máster de formación permanente online en ciberseguridad	Information security	EQF7 (master)	Mondragón Unibertsitatea	Private	https://www.mondragon.edu/cursos/es/master-ciberseguridad	Degree	10	50	Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad / Master in Cybersecurity	Cyberdefense	EQF7 (master)	Universidad de Murcia	Public	https://www.um.es/web/estudios/masteres/ciberseguridad	Degree	10	50	Official 90 ECTS online
Spain	Máster Universitario en Ciberseguridad	Ethical Haking	EQF7 (master)	UNED	Public	https://www.uned.es/universidad/inicio/estudios/masteres/master-universitario-en-ciberseguridad.html	Degree	47	75	Official 60 ECTS semi campus and online

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete programme (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	Máster Universitario en Ciberseguridad y Privacidad / Cybersecurity and Privacy	Data proteccion	EQF7 (master)	Universitat Oberta de Catalunya	Private	https://www.uoc.edu/es/estudios/masters/master-universitario-ciberseguridad-privacidad	Degree	83		Official 60 ECTS online
Spain	Máster Universitario en Ciberseguridad / Master in Cybersecurity	Information security	EQF7 (master)	Universidad Politécnica de Catalunya	Public	https://www.upc.edu/ca/masters/cybersecurity	Degree	20	44	Official 60 ECTS campus
Spain	Máster Universitario en Ciberseguridad	Information security and cybersecurity	EQF7 (master)	Universidad Politécnica de Madrid	Public	https://www.upm.es/Estudiantes/Estudios_Titulaciones/Estudios_Master/Programas?id=9.19&fmt=detail	Degree	20	25	Official 60 ECTS campus
Spain	Máster Universitario en Ciberseguridad y Ciberinteligencia	Cybersecurity and Cyberinteligence	EQF7 (master)	Universitat Politècnica de València	Public	https://www.upv.es/titulaciones/MUCC/indexc.html	Degree	9	30	Official 90 ECTS semi campus and online
Spain	Graduado o Graduada en Ingeniería de la Ciberseguridad	Cybersecurity, information security	EQF6 (bachelor)	Universidad Rey Juan Carlos	Public	https://www.urjc.es/universidad/calidad/3100-ingenieria-de-la-ciberseguridad	Degree	23	60	Official 240 ECTS campus
Spain	Máster Universitario en Ingeniería de la Seguridad Informática e Inteligencia Artificial	Cybersecurity, information security	EQF7 (master)	Universidad Rovira i Virgili	Public	https://www.iu.org/master/cyber-security/	Degree	16		Official 120 ECTS online

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete program me (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	Graduado o Graduada en Ingeniería de la Ciberseguridad	Cybersecurity, information security	EQF6 (bachelor)	Universidad San Jorge	Private	https://www.usj.es/estudios/grados/ingenieria-ciberseguridad	Degree	23	50	Official 240 ECTS campus
Spain	Máster Universitario en Ciberseguridad	Cybersecurity, information security	EQF7 (master)	Universidad de Vigo	Public	https://www.uvigo.gal/es/node/247124	Degree	89	0	Official 90 ECTS campus
Spain	Máster en Ciberseguridad (Presencial con Deloitte)	Ethical Haking	EQF7 (master)	IMF Smart Education	Private	https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica-presencial	Degree			Non official campus
Spain	Máster Ciberseguridad en Hacking Ethico: Redes CCNA + CiberOps + Fortinet	Ethical Haking	EQF7 (master)	Tajamar	Private	https://fpprofessionaleducation.tajamar.es/ciberseguridad-en-redes/	Degree			Non official campus
Spain	Certified Ethical Hacker	Ethical Haking	EQF5 (associate degree)	It Institute	Private	https://es.it-institute.org/ceh-certified-ethical-hacker/	Certificate			Non official online
Spain	Ciberseguridad en Redes: CCNA + CyberOps + Fortinet	Ethical Haking	EQF5 (associate degree)	Tajamar	Private	https://fpprofessionaleducation.tajamar.es/ciberseguridad-en-redes/	Diploma			Non official online and campus
Spain	Cybersecurity Operations - Cisco Certified CyberOps Associate (CBROPS)	Cyberdefense	EQF5 (associate degree)	PUE	Private	https://www.pue.es/cursos/cisco/200-201-cyberops-associate	Certificate			Non official

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete program me (2021-2022)	# possible learners (p. year)	Other relevant information
Spain	MASTER PROPIO EN DATA, COMPLEX NETWORKS & CYBERSECURITY SCIENCES	Cybersecurity management	EQF7 (master)	Universidad Rey Juan Carlos	Public	https://www.urjc.es/component/k2/4363-data-complex-networks-cybersecurity-sciences	Degree		50	Non official campus and online
Spain	Gestión de la Ciberseguridad	Cybersecurity management	EQF5 (associate degree)	Universidad Francisco de Vitoria	Private	https://www.ufv.es/plan-de-estudios-grado-en-gestion-de-la-ciberseguridad/	Degree			Non official
Spain	Ingeniería de la Ciberseguridad	Cybersecurity, information security	EQF6 (bachelor)	Universidad Rey Juan Carlos	Public	https://www.urjc.es/universidad/calidad/3100-ingenieria-de-la-ciberseguridad	Diploma		60	Non official 240 ECTS campus
Spain	Bootcamp de ciberseguridad	Ethical Haking	EQF5 (associate degree)	Ironhack	Private	https://www.ironhack.com/es/ciberseguridad	Diploma			Non official campus and online
Spain	Programa experto en ciberseguridad empresarial	Cybersecurity management	EQF5 (associate degree)	Schiller International University	Private	https://sibt.schiller.edu/formacion/programa-experto-en-ciberseguridad-empresarial/	Diploma			Non official campus
Spain	Master en Redes y Ciberseguridad	Cybersecurity, information security	EQF7 (master)	CESTE, Escuela Internacional de Negocios	Private	https://www.ceste.es/programas/mrc-master-en-redes-y-ciberseguridad/	Degree			Non official 90 ECTS campus and online
Spain	Máster Executive en Ciberseguridad Manager	Cybersecurity management	EQF7 (master)	Digital Age University	Private	https://digitalageuniversity.com/program/master-in-cybersecurity-manager/	Degree			Non official
Spain	Maestría en Ciencias de la Computación - Ciberseguridad,	Cybersecurity, information security	EQF7 (master)	MIA Digital University	Private	https://miauniversity.com/en/master/master-in-computer-science-cybersecurity-data-	Degree			Non official online

Country	Title	Specialisation	Level	Provider	Type of institution	Link	Recognition	# learners complete programme (2021-2022)	# possible learners (p. year)	Other relevant information
	Análisis de Datos e IA					analytics-and-artificial-intelligence/				
Spain	Master en Ciberseguridad	Cybersecurity management	EQF7 (master)	Euroinnova International Online Education	Private	https://www.euroinnova.edu.es/master-ciberseguridad-online	Degree			Non official 60 ECTS online

Co-funded by
the European Union

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