

SPAIN CYBERSECURITY MARKET FOR THE VIRGINIA ECONOMIC DEVELOPMENT PARTNERSHIP



| MARKET RESEARCH

VEDP

Virginia
Economic
Development
Partnership



INDEX

INTRODUCTION	pg. 01
SUMMARY	pg.02-03
MARKET SIZE	
Turnover	pg.04
Number of companies & geographical concentration	pg.04
Threats & incidents	pg.05-07
MARKET TRENDS	
COSTS	
PUBLIC INVESTMENTS, CONTRACTS AND TENDERS	
Government investment & European recovery funds	pg.13-15
Tender analysis	pg.16-17
Detailed analysis of tenders	pg.18-20
STANDARDS AND CERTIFICATIONS	
Laws	pg.21-24
Standards	pg.25
STATUS OF CYBERSECURITY IN KEY SECTORS	
Financial sector	pg.26-27
Energy	pg.28-29
Health Sector	pg.29-32

MAJOR PLAYERS

Largest clients in each sector pg.34-37

Main IT integrators pg.37-41

Leading cybersecurity and MSSPs pg.42-44

Other companies pg.44

Public institutions pg.45-47

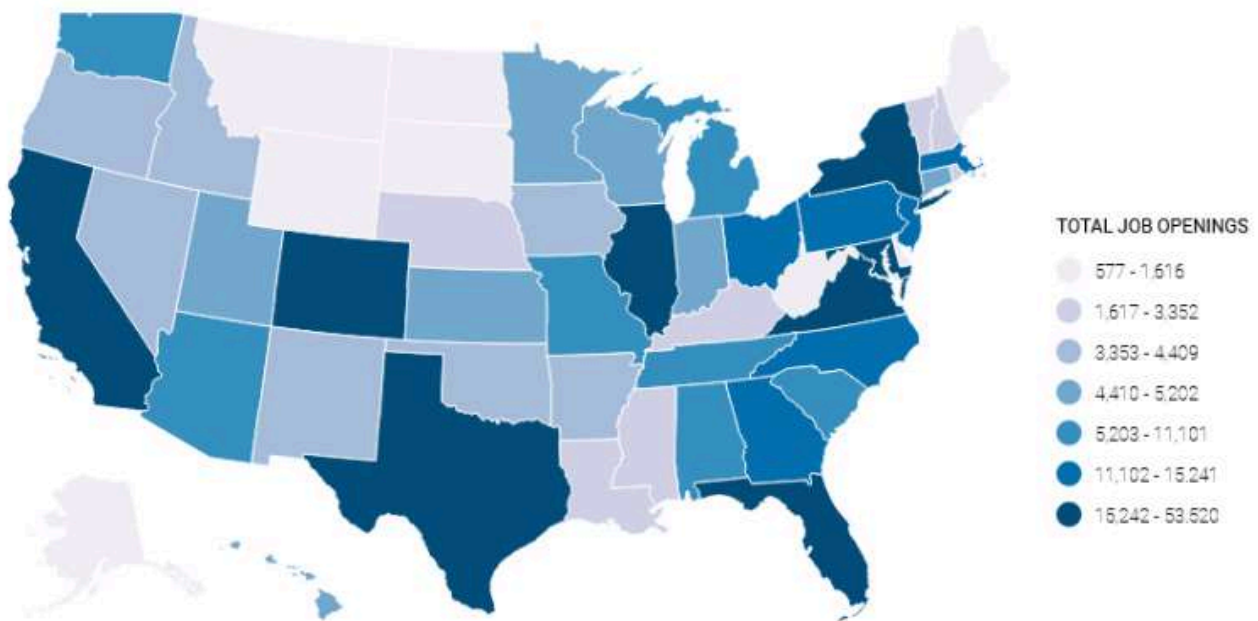
Business associations pg.47

INTERNATIONAL EXPANSION

TRADE FAIRS AND EVENTS

01. INTRODUCTION: CYBERSECURITY IN VIRGINIA

Virginia is a leader in the cybersecurity sector, offering more cybersecurity job openings than any other state in the US.



Source: Cyberseek¹

It has the second strongest cybersecurity industry, with the second largest workforce, in the US. The industry benefits from the proximity to Washington DC, providing it with access to the headquarters of security institutions, armed forces, and many other critical agencies. The state is a leading adopter of state-of-the-art cybersecurity politics. For example, it was the first state to adopt the National Institute of Standards and Technology (NIST) Cyber Framework and to declare itself an Information Sharing and Assessment Organization. (ISAO) With the support of VEDP, Virginia's cybersecurity industry has entered foreign markets and become a critical supplier all around the world

1. [Cybersecurity Supply And Demand Heat Map](#). The data is provided by the Computing Technology Industry Association and the National Institute of Standards and Technology (NIST).

02. SUMMARY

The Spanish cybersecurity sector offers an attractive trading opportunity to American suppliers offering expertise once they understand how to navigate some complexities in the tender process and regulatory framework. At approximately 2 billion euros a year and a 10% annual growth rate, Spain boasts a large market. Researchers show that in global comparison, most revenue will be generated in the United States

Recent events, ranging from the pandemic to large increases in cybersecurity incidents to Russia's invasion of Ukraine, have dramatically increased the profile of cybersecurity in Spain. Thus, the present moment offers an opportunity, as Spanish businesses are increasingly willing to invest in cybersecurity and to pay more for services/products with technical advantages. While such investment faces challenges due to the high level of European regulatory hurdles and complicated processes for tenders, American companies with effective advice from Spanish organizations could still make competitive suppliers. Additionally, given Spain's ties to Latin America, selling in Spain will open sales in the whole Latam.

Market size: Approximately 2 billion euros a year, with an annual growth rate close to 10%. This growth rate presents an opportunity for suppliers.

Number of Spanish companies: approximately 1,800. High geographical concentration in Madrid and Barcelona.

There is **high awareness about cybersecurity** in the Spanish market. This awareness is growing and has been further boosted by the Russian invasion of Ukraine.

Ransomware and malware are the top cybersecurity priority for Spanish businesses at the moment.

Spain is a decentralized country where regional governments have ample competencies in multiple areas. However, Spanish regions have not invested heavily in cybersecurity, and most of the 17 regional governments don't have any specialized cybersecurity agency.

The Spanish cybersecurity has wide presence in the Latin American market. Becoming a supplier to a relevant Spanish multinational may provide access to large markets and clients in Latin America. Spain is the second largest investor in Latin America where Spanish businesses have an advantage due to shared language, some cultural similarities and reputation.

The Spanish administration procures a large volume of cybersecurity services through public tenders. There is no centralized purchasing body due to the decentralized nature of the Spanish administration. The Spanish Cybersecurity Institute (INCIBE), the Defense Ministry and Army, the regional cybersecurity agency of Catalonia, the Social Security Institute, are the managing agencies for important infrastructures (rail, airports, roads).

Institutions procure cybersecurity services for their own use (protecting the government's systems) and to provide to private organizations (incentive and promotion programs that subsidize businesses to get cybersecurity services). **Both types of investment offer opportunities to foreign suppliers.** They can become suppliers to the Spanish administration, and to Spanish SMEs by participating as providers in government-funded programs (i.e Kit Digital)

Cybersecurity is an investment priority for the EU, within its larger goal of digital transformation. Many Spanish public programs are financed with European funds, and more funding will be provided in the future.

Almost all tender winners are companies with an office in Spain. While public tenders are almost always open to foreign companies, entering and winning one is difficult for them due to procedural complexity, the lack of insider market knowledge, and the necessity of submitting in Spanish. Instead it's recommended to become a supplier/partner to a local company that enters the tenders.

The GDPR, the privacy regulation in the EU, includes important cybersecurity requirements for companies that keep personal data. European authorities consider American law to provide inadequate protection for personal data. Accordingly American companies would need to prove that they meet these protection standards in order to work with European personal data.

Spain has a National Security Scheme, similar to American CMMC, that defines cybersecurity measures (technical and organizational) that companies will eventually have to comply with to exchange data with the Spanish administration. This means that CMMC expertise may not necessarily be a competitive advantage for an American supplier in the Spanish market.

Cybersecurity costs are lower in Spain than in North America. Senior workers in Spain may charge up to 80 dollars an hour. Mid range consultants may be paid 43,000 dollars a year (+33% social security), and managers with 15 years of experience may be paid up to 88,000 dollars a year (+33% Social security). Thus, competing in price may not be the best strategy for American companies in Spain; it may be better to compete in quality and differentiation. Likewise it could be an opportunity to partner with a Spanish company with lower cost to enter new markets in Europe.

Market leaders include a mixture of business consultancy firms, IT consultancy firms, and cybersecurity specialists, both Spanish and foreign multinationals.

03. MARKET SIZE

Turnover

According to several market research companies, **the cybersecurity market in Spain has a value close to 2 billion euros a year.**

According to DBK,² the revenue of the cybersecurity market (including hardware and software) in Spain was **1.9 billion euros in 2022**. This marks a 30% increase from 1.5 billion in 2020.

IDC Research³ expects a market revenue of 2.1 billion euros in 2023, and the government predicts the sector to grow at an annual rate of nearly 15% in the coming years. Statista predicts 2.8 billion euros of revenue in 2024.

General ICT consultants offering cybersecurity services account for the majority of this revenue - 72%. The rest is generated by cybersecurity specialists.

According to sector sources, this is due to the fact that large cybersecurity projects are carried out by systems integrators: general IT companies that integrate systems and services from multiple suppliers, providing turnkey solutions to the client.

Number of companies and geographic concentration

As of March 2023, DBK had identified **1,854 companies offering cybersecurity services**. INCIB, the government's institute for cybersecurity, lists 1,700 companies in its online directory.

The Spanish ICT sector is characterized by **high geographical concentration**. Most ICT companies are concentrated in the autonomous communities of Madrid (33%) and Catalonia (22%) - specifically in the **Madrid and Barcelona metropolitan areas**.

This concentration is especially apparent when considering company size. Metropolitan areas, especially Madrid, not only concentrate a greater number of companies, but are also the main headquarters of the largest companies in the sector. Accordingly, large companies in Madrid account for more than half of the sector's revenue, investment, personnel, and clients.

2. [Ciberseguridad | Nota de prensa 2023 | DBK Observatorio Sectorial](#), March 2023.

3. [Tendencias de ciberseguridad en 2023 | OPINIÓN | CSO España](#), January 2023.

Threats and incidents

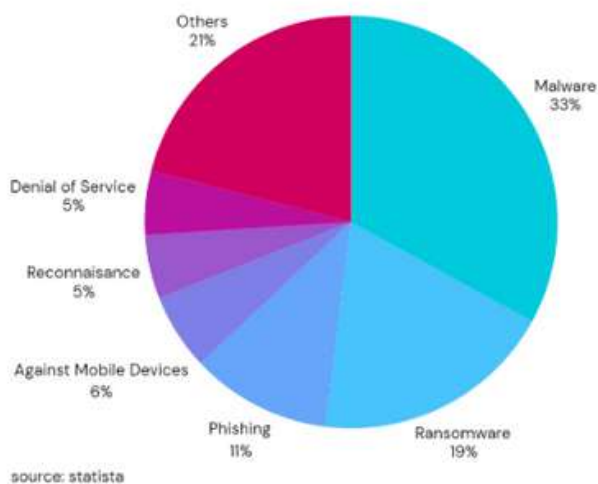
The Spanish government's Cybersecurity Institute (INCIBE) managed **83,517 cybersecurity incidents in 2023**: a 24% increase from the previous year.⁴

More than 58,000 of these attacks affected citizens (Internet users) and the rest - over 22,000 - affected private companies, including SMEs, micro-SMEs and the self employed.

237 incidents affected essential and critical operators. These companies or services, which are indispensable for the proper daily functioning of society, include the following sectors:

- 25.42% to financial and tax systems.
- 25% to transportation
- 22.08% to energy
- 18.33% to Information and Communication Technologies (ICT)
- 4.58% to water infrastructure

The nature of the attacks was as follows:

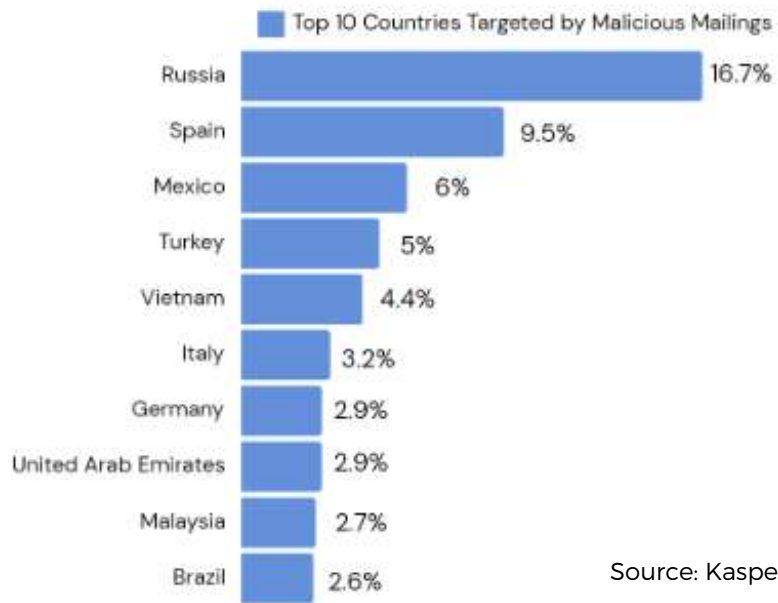


Other details about the incidents include the following:

- Over 9,000 compromised devices
- 28,000 fraud cases
- 7,000 websites hosting abusive
- 237 incidents in key sectors like finance, transportation, energy, IT, and water services
- Over 310 fraudulent online stores closed
- 26,200 virus-related cases, including 621 ransomware attacks
- 80,920 inquiries on identity theft, cyberbullying, phishing attempts, and fraudulent online activities

4. [Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior.](#) April 2024

According to Kaspersky’s 2023 cybersecurity statistics, Spain ranked as the second most targeted country by malicious mailings, affecting 9.5% of its users:



Source: Kaspersky

Spain also ranked fourth among the most attacked countries by cyberthreats, with 2.23% of its users targeted

	Countries and territories*	%**
1	France	2.41
2	China	2.38
3	Italy	2.38
4	Spain	2.23
5	United States	2.16
6	India	2.16
7	Mexico	2.12
8	Canada	1.99
9	Australia	1.85
10	Great Britain	1.84

Source: Kaspersky

In the Global Cybersecurity Index published by the International Telecommunication Union, Spain is the 4th world country with the highest cybersecurity commitment, and the second in the European Union. This index aggregates a variety of statistical indicators along with other indexes, assessing countries and organizations. These indicators measure aspects such as cyber maturity, incidents, regulations, and cybersecurity investments, among others.

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5

In May 2024, there was a wave of cyberattacks targeting major Spanish companies listed on the Ibex 35, Spain's principal stock exchange, including Banco Santander, Telefónica, and Iberdrola.⁵ These attacks compromised user data but largely avoided accessing highly sensitive information. Santander reported unauthorized access to a database containing information on clients and employees. Telefónica faced a data breach affecting 120,000 users, while Iberdrola exposed data of 850,000 customers. Additionally, Spain's Directorate General of Traffic (DGT) suffered a cyberattack, compromising the data of over 30 million drivers.

Cyberattacks have tripled compared to 2022, with the financial, transportation, and energy sectors being primary targets. Digital transformation and the use of new technologies like AI are contributing factors to these attacks. Cybercriminals are increasingly exploiting the weakest links in the supply chain, often targeting smaller providers and users.

5. [Los 'hackers' disparan contra el Ibex 35: ¿qué hay detrás de estos ciberataques? - Bolsamania.com](#), June 2024

03.

MARKET TRENDS

Deloitte, one of the leaders in the Spanish cybersecurity market, conducts a yearly survey on cybersecurity in Spain. The survey is focused on the major players in four priority sectors: energy, finance, healthcare and public administration, with an overrepresentation of big companies (50% of the respondent companies have more than 1,000 workers). The following are relevant findings from the 2024 edition:

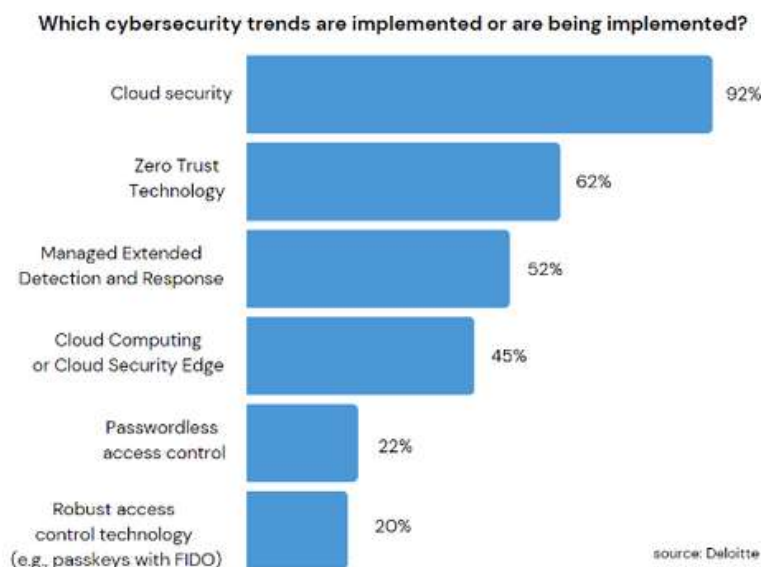
- **Outsourcing:**
 - 86% of the organizations outsource most of their cybersecurity tasks.
 - 66% of the cybersecurity budget is spent on outsourced services, and 68% of the respondents outsource more than half of their cybersecurity staff.
 - However, most companies don't have comprehensive control measures of their outsourcing providers; this control is considered difficult and costly.
- Cybersecurity **budgets** have had several consecutive years of sustained growth, in the 3-6% range every year for outsourced staff. Only 2% of the organizations have decreased their cybersecurity budget recently.
- **Incidents:**
 - Incidents keep getting more frequent: only 10% of the respondents say that they have experienced a reduction in the number of incidents in the last year.
 - The main cybersecurity challenge, for 82% of the companies, is the increasing sophistication and budget of the attackers.
 - Ransomware is the main attack that worries the companies.
 - 70% of the companies have only approximate ideas of the cost that cyberattacks cause.
- Only 2% of the companies have full trust on their cybersecurity measures.
- Companies are late to **AI cybersecurity**: a specific AI cybersecurity strategy is missing in 51% of the companies.
- The main **cybersecurity frameworks** used in Spain are: ISO 27001 (70%), Deloitte CSF (45%), NIST CSF (43%) and MITRE (28%). MITRE, in particular, has seen recent growth.

Certifications and standards are very important in the market.

Cybersecurity is a critical area, where problems can compromise company activity, but it is also a relatively new and very specialized field. Thus, most companies outsource many or all their cybersecurity activities. Clients utilize certifications and standards to ascertain the capability and quality of suppliers.

The Russian invasion of Ukraine is raising cybersecurity’s profile in Spain. Authorities have warned that cyberattacks to companies and government systems have been growing since January 2022, often attributed to Russian groups. A leading government official in cyberattack prevention revealed in 2023 they detected 50-60 severe attacks on government networks and 200-300 on private companies annually, 45% originating from Russia.⁶

Companies highlight several **trends** that are relevant today and in the short term. Cloud security leads adoption, indicating a strong commitment to securing data and applications in cloud environments. Zero Trust technology follows closely, emphasizing stricter access controls and continuous verification processes. Managed Extended Detection and Response (MXDR) is gaining traction, highlighting integrated monitoring and response capabilities against sophisticated cyber threats. Additionally, passwordless access control technology is becoming prominent, reflecting a strategic move to enhance security by reducing reliance on traditional passwords vulnerable to breaches and phishing attacks.



6. El CNI apunta a Rusia: «España está sufriendo ciberataques de peligrosidad crítica». March 2022

A recent "Voice of the CISO" report by Proofpoint⁷ highlights significant concerns among Chief Information Security Officers (CISOs) in Spain regarding cybersecurity. The survey shows a sharp increase in apprehension, with 72% fearing a major cyberattack in the next year, up from 31% last year. Additionally, 64% feel their organizations are unprepared for targeted cyberattacks, compared to 49% last year.

Internal threats, email fraud (BEC), and supply chain attacks now top their concerns, replacing ransomware and cloud breaches from previous years. Despite facing data losses, partly due to employee turnover, 51% of CISOs believe their current data protection measures are adequate. However, 64% note economic instability has negatively impacted their cybersecurity budgets, potentially limiting resources.

Regarding ransomware, 64% anticipate their organizations would consider paying to restore systems and prevent data exposure. Additionally, 65% would seek cyber insurance to mitigate losses. Human error remains critical, cited by 65% of CISOs, though 73% believe employees understand their security role, up from 53% last year, reflecting efforts to enhance security culture.

The Global Cybersecurity Leadership Insights 2023 report by EY⁸ highlights that only 20% of Chief Information Security Officers (CISOs) consider their organization's cybersecurity strategies effective. This indicates widespread challenges in global cybersecurity, underscored by an average of 44 incidents per organization annually, each with significant financial implications. Despite substantial investments, averaging \$35 million per organization annually, the average cost of security breaches rose by 12% to \$2.5 million in 2023, revealing the inadequacy of current measures in mitigating risks.

The prominence of the CISO role has markedly increased in recent years, catalyzed by rapid technological advancements and intensified by the COVID-19 pandemic. The pandemic accelerated digital transformation efforts, compelling organizations to adapt their technological profiles and security strategies to accommodate remote work and evolving market dynamic.

7. [El 72% de los CISO en España teme sufrir un ciberataque importante](#) | Seguridad | IT Reseller. May 2023

8. [Cyber leaders' confidence in their organization's defenses plummets, but costs mount](#) | EY - Global

04. COSTS

Cybersecurity costs and wages are among the highest in the Spanish IT sector. We have compiled several sources that provide a price range for cybersecurity. The following costs include both wages and social security contributions.

Comparing these costs with the equivalent positions in the USA leads to the conclusion that a labor-intensive American company will need very strong differentiation **to be competitive in the Spanish market.**

The government program for EU COVID recovery funds (Next Generation EU) includes a cybersecurity component that provides **reference costs** for companies seeking to provide cybersecurity services to the Spanish public administration.

Position	Hourly cost (euros)	Hourly cost (USD)
Cybersecurity Project Manager	73	81
Cybersecurity Governance and Regulation Consultant	60	66.61
Risk and Compliance Consultant	48	53.29
Cybersecurity Architect	60	66.61
Cybersecurity Systems Administrator	45	50
Security Auditor	45	50

Source: Recovery, Transformation and Resilience Plan, Component 11.

An international labor cost survey performed by Roger Walters provides several **reference salaries** for Spain, according to their years of experience:

Position	Labour cost by years of experience			
		3 to 7	7 to 15	15+
Application Security Specialist	€	53,000 - 67,000	67,000 - 80,000	88,000 - 107,000
	\$	56,940 - 72,000	72,000 - 94,550	94,550 - 87,859
Cybersecurity Manager	€	80,000 - 91,000	88,000 - 107,000	-
	\$	94,550 - 97,770	94,550 - 87,859	-

We have researched job offers that demand knowledge of the ENS framework, which is more or less similar to the American CMMC.

Position	Cost range (euros per year)	Cost range (dollars per year)
Risk Consultant	40,000+	43,040+
Security Engineer	52,300+	56,260+
Senior Consultant	40,000 - 52,000	43,040 - 55,950

05. PUBLIC INVESTMENTS, CONTRACTS AND TENDERS

Government investment and European recovery funds

The Spanish government and other Spanish administrations are responsible for multiple investments in the cybersecurity sector:

- Incentive programs oriented to large companies and SMEs, and to other private institutions, to help them improve their cybersecurity measures.
- Direct investment and expenditure by the administrations to implement cybersecurity in their own information systems.

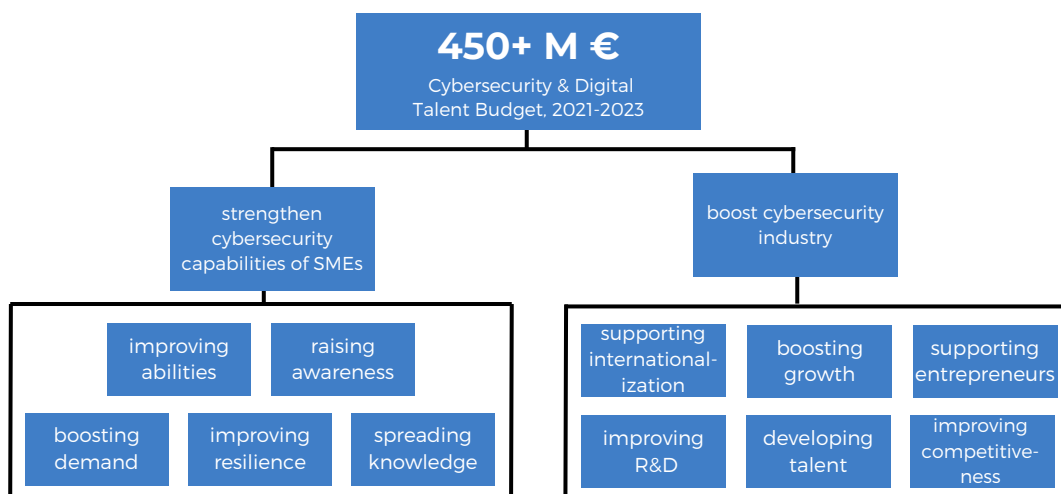
There are three levels of government in Spain: national, regional (constituted of 17 “Autonomous Communities,” or states), and local (constituted of 8,131 city councils, 50 provinces, and 2 autonomous cities). Spain is a relatively decentralized country, and regional governments have a high degree of control in important areas of policy, such as healthcare and education.

The administrative divisions means that **there are no centralized buyers of cybersecurity services.** Rather, all of these subnational governments, as well as their ministries, departments, agencies, public companies, and other organizations, may purchase cybersecurity services directly and independently. There is not a single cybersecurity “budget” for the Spanish administration, and it may be difficult to know how much money the government has committed to this goal, since there are many administrations, with many programs they manage on their own or jointly, and that may overlap each other.

The following are some recent investment, expenditure, and incentive programs to show current priorities.

European recovery plan (Next Generation EU): After the COVID crisis, the EU launched its largest investment plan ever to promote recovery. This plan covers many areas, but there are two main goals: climate action and digital transformation. The plan will continue until 2027. Spain has budgeted 4.3 billion euros of cybersecurity investment within this plan. Some of the following actions are partly financed with EU recovery funds.

Digital Agenda 2025: This large-scale plan for the digital transformation of businesses includes 450 million euros of incentives for cybersecurity projects from 2021 through 2024. A large part of this has been funded by the European Union’s COVID-19 recovery plan. INCIBE is the agency responsible for assessing and managing cybersecurity projects.⁹ The activity areas for eligible projects include:



It is important to note that Spain has a high number of SMEs, which generally lag behind larger companies in terms of cybersecurity. These companies don’t have great investment capacity: to implement new technology, they need low-cost, standardized solutions and a great deal of outsourcing. **This is an opportunity for suppliers who are cost-efficient and can compete in this segment.**

9. Incibe será «brazo ejecutor» del plan industrial de 450 millones de euros para la ciberseguridad en España. Leonoticias. April 2021.

Another relevant aspect of the European recovery funds is that they promote further digitization and technology implementation across multiple sectors and for various uses: for example, IoT, smart cities, smart energy grids, industry 4.0 and the digitization of small and medium enterprises. This is going to increase the scope of activities that cybersecurity must protect, and thus create new sources of demand.

National Cybersecurity Plan: In 2022, the Spanish government approved a National Cybersecurity Plan until 2025, with 150 actions and an estimated budget over **1.2 billion euros**. A large part of this plan was to be financed with European funds for recovery and economy transformation after COVID.

Among the main actions of the National Cybersecurity Plan, the highlights include:

- The creation of the national platform for the notification and monitoring of cyber incidents and threats, allowing real-time information exchange between public and private entities.

- Promoting the implementation of the Cybersecurity Operations Center for the General State Administration and its Public Bodies.
- The development of an integrated system of cybersecurity indicators at the national level.
- Increasing the creation of cybersecurity infrastructures in autonomous communities, cities, and local entities.
- Enhancing cybersecurity for SMEs, micro-enterprises, and self-employed individuals.
- Promoting a higher level of cybersecurity culture.

Additionally, the plan includes the creation of a monitoring and control system to identify the degree of implementation of the measures and to issue an annual evaluation report.

Activa Ciberseguridad: This is a 10 million euro incentive program, started in 2022, aimed at SMEs, that provides free consulting in the field of cybersecurity. Experienced suppliers assess each company's situation and prepare an action plan to improve the company's security

Activa Ciberseguridad

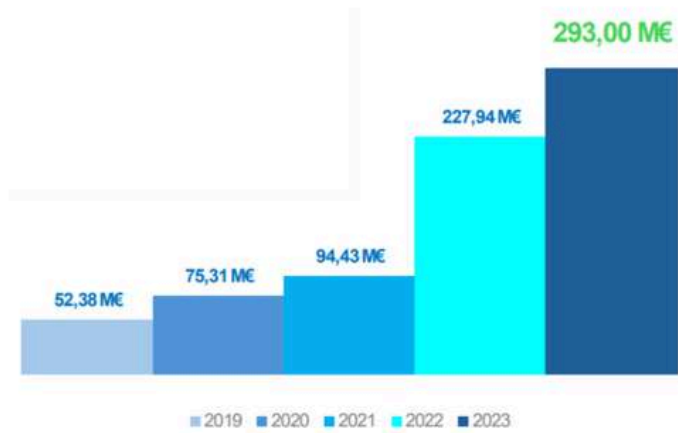


Financiado por
la Unión Europea
NextGenerationEU



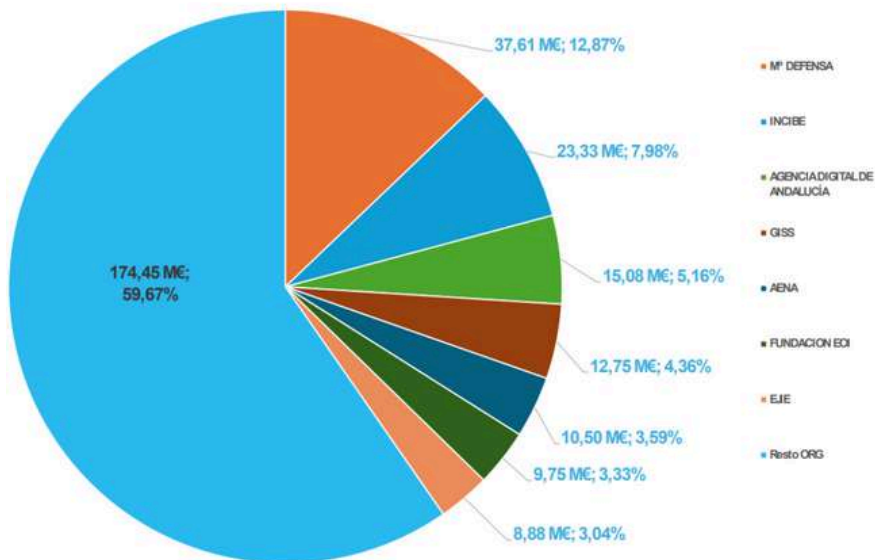
Tender analysis

Basic summary of tenders: The evolution of Spanish public cybersecurity tenders over the past five years shows a remarkable growth of 463% from 2019 to 2023.



Source: AdjudicacionesTIC

The top institutions by cybersecurity expenditure and investment are the following:



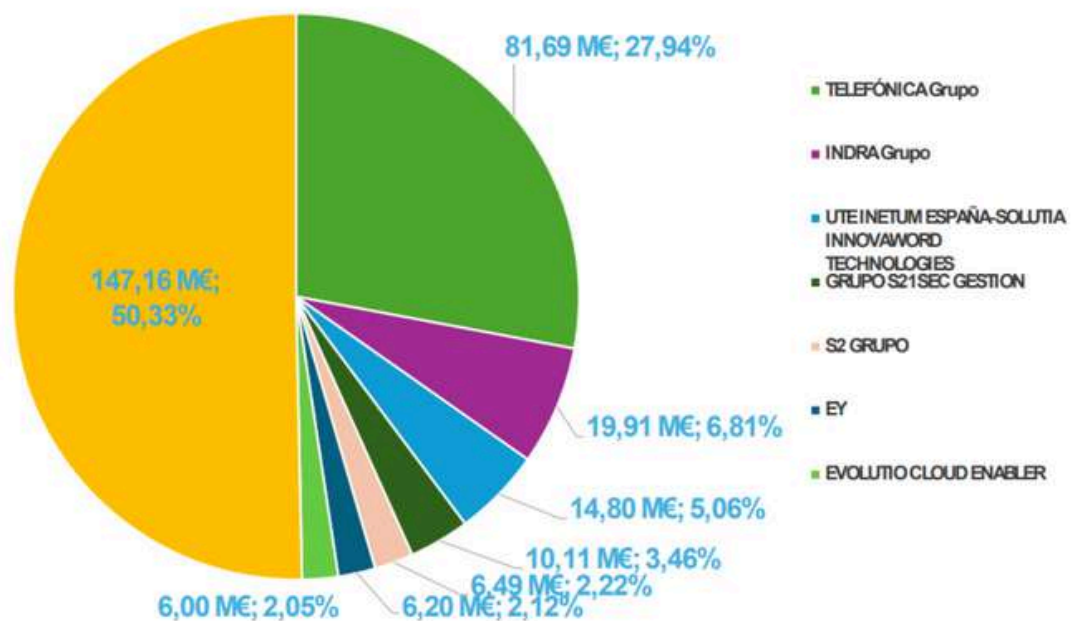
Source: AdjudicacionesTIC

This breakdown is interesting because it shows institutions involved in very different areas and from different administration levels:

- Ministry of Defense: Spanish army and national armed forces.
- INCIBE: national Spanish cybersecurity institution.
- Agencia Digital de Andalucía: regional ICT promotion institution for Andalusia.
- GISS: technology department for the Spanish social security (national, dependent on a ministry).
- AENA: government-owned company managing airport infrastructure.
- EOI: government-owned business school that manages many programs for business education.

Among the 90 companies that received one of the more than 150 contracts, the distribution reveals that the top 7 contractors collectively account for nearly 50% of the total.

Telefónica Group leads with the largest amount of contracts awarded, totaling €81.69 million, followed by Indra Group with €19.9 million, and then the Joint Venture (UTE) formed by Inetum Spain and Solutia Innovaword Technologies with €14.80 million.



Source: AdjudicacionesTIC

Detailed Analysis

We have analyzed **a sample with over 780 tenders**, from October 2022 to June 2024. This sample does not include all the cybersecurity RFPs published in Spain during that period, for two reasons: there isn't a specific classification code for cybersecurity, which means that we have to perform term searches through description text; and while the central portal is the largest in Spain, not all government bodies publish their tenders there, but some use their own portals. Also, we have only reviewed tenders over 100,000 euros.

The sample includes:

- More than 780 tenders with a total budget of 1.5 billion euros.
- More than 450 tenders that are available on the Spanish government's central tender portal, allowing further analysis.
- 341 tenders that have already been awarded, with a value of 420 million euros.
- The maximum budget reaches almost 100 million euros.
- 115 tenders over 1 million euros during that period.
- 120 individual winning companies.
- 30 winning groups that have temporarily joined for specific tender.

A very important conclusion is that we haven't identified any foreign company that has won these tenders.

The leading company, far beyond the others in number of awarded tenders, is Telefónica. Other relevant companies, either by total awarded amount or by number of wins, are: Nunsys, MTP, Indra, S21SEC, NTT Spain, Indra-SIA, Accenture, ICA Sistemas.

The governmental organizations that have published more RFPs include the following:

- Spanish National Cybersecurity Institute (INCIBE)
- Catalanian Cybersecurity Agency
- Technology Department of the Spanish Social Security Institute
- Renfe (public rail service operator)
- ISDEFE (public company providing services to the Spanish armed forces)
- Defense Ministry
- AENA (public airport infrastructure operator)
- DGT (traffic control authority)
- Technology agencies in the regional governments of the Canary Islands, Galicia, Madrid, Murcia, Asturias

Strategy for participating in tenders

While public tenders are almost always open to companies from other countries, in practice **all the tenders we have reviewed have been won by Spanish companies** (even if some of them are subsidiaries of foreign multinationals).

The explanation for this is simple. **Even if there's no discrimination for foreign companies, entering a public tender in Spain is a complex affair.**

Government organizations of all administrative levels (national, regional and local) are obliged to manage their procurement of products and services through a standardized public tender process. The system is organized according to EU laws, and its advantages are that it's standard, transparent and has built-in procedures to prevent corruption. All services contracts for more than 15,000 euros need to undergo the tendering process.

On the other hand, **the tendering process is complex and quite demanding for the participating companies.** Non EU companies are allowed to submit offers to tenders in equal conditions, in general (though tenders related to police and security might be an exception and not be open). However, in practice, the complexity of the tendering process makes it hard for foreign companies to compete:

- **Submission system:** The proposal must generally be submitted through an specific secure system that demands identity certificates.
- **Documentation:** The proposal must include a large number of documents separated in several groups, following strict rules about what information cannot be included in each group, and rules about the contents and validity of each document.
- **Language:** The submission language is almost always Spanish with no possibility to submit an offer in English, and the RFPs are published in Spanish as well (though they may be totally or partially translated for dissemination in the European Tenders Daily platform); in some cases (when submitting to specific regional organizations), Spain's co-official languages may be required too (Galician, Catalan or Basque).
- **Deadlines:** The deadlines for the tendering process depend on the complexity of the request. 1-month deadlines are quite common.

This means that **the formalities are quite demanding for a non-Spanish company.**

Besides that, there is a subjective element of **market knowledge**: understanding the role of the public organization that has published the tender and its goals, and being able to tailor the proposal beyond what is merely specified in the RFP. This is even harder for a company without a Spanish office.

And, in some cases, the tender includes requirements that are harder for foreign companies. Not specific nationality requirements like “the bidder must be a company registered in Spain,” but experience requirements like “the bidder must have obtained a certification for the Spanish National Security Scheme” or “the staff must have knowledge of specific tools provided by Spanish institutions like the National Cryptology Center.”

Special legal requirements for cybersecurity may also make it difficult for non-EU companies (see chapter on regulations).

For these reasons, the **recommendation** to enter a cybersecurity tender in Spain is to become a supplier and partner to a Spanish provider who is used to participating in such tenders.

Most of the tenders published in Spain are managed through a central repository located at contrataciondelestado.es. However, the contracting authorities are free to use this centralized service or roll their own, and some regional governments like Catalonia, Andalusia, and the Basque Country publish their own tenders in their own platforms.

06.

STANDARDS, CERTIFICATIONS AND REGULATIONS

Laws

NIS 2 Directive: The Network and Information Security Directive, known as NIS 2 (Directive (EU) 2016/1148), is a European Union regulation¹⁰ aimed at enhancing cybersecurity preparedness and resilience across member states. It mandates enhanced cybersecurity measures for several critical industries:

- Operators of Essential Services (OES):
 - Postal and courier services
 - Waste management
 - Chemicals
 - Food
 - Manufacturing of medical devices
 - Financial market infrastructures
 - Drinking water supply and distribution
 - Computers and electronics
 - Machinery equipment
 - Motor vehicles
 - Energy
 - Transport
 - Banking
 - Healthcare
- Digital Service Providers (DSPs)
 - Online marketplaces
 - Cloud computing services
 - Search engines
 - Digital infrastructures

These entities must implement security measures and report significant cyber incidents to national authorities. The directive affects all suppliers that provide digital services or are part of critical infrastructure in EU member states. Compliance is required if they serve EU-based customers or operate within EU jurisdictions under the directive's scope. Compliance varies based on national implementations and sector-specific regulations within EU member states.

Non-EU entities providing specific digital services within these sectors must appoint a representative in an EU Member State where services are offered. This representative ensures compliance with the directive's requirements. Without a representative, any EU Member State where services are provided can take legal action against the entity for non-compliance with the directive.

10. [Directive on measures for a high common level of cybersecurity across the Union \(NIS2 Directive\)](#)

EU Critical Entities Resilience Directive

Effective from January 16, 2023, this directive¹¹ mandates member states to identify critical entities across eleven sectors by July 17, 2026. These sectors include:

1. **Energy sector**, with electricity production and energy storage services.
2. **Transport sector**, with management and maintenance of airport or railways infrastructure services.
3. **Banking sector**, with essential services like taking deposits and lending.
4. **Financial market infrastructure sector**, with services such as the operation of trading venues and clearing systems.
5. **Health sector**, with distribution, manufacturing, provision of healthcare, and medical services.
6. **Drinking water sector**, with supply and distribution.
7. **Wastewater sector**, with collection, treatment, and disposal services.
8. **Digital infrastructure sector**, with services such as the provision and operation of internet exchange points, domain name systems, top-level domains, cloud computing, and data centers.
9. **Public administration services**
10. **Space sector**, with the operation of ground-based infrastructure services
11. **Food production, processing, and distribution sector**, with large-scale industrial production and processing, supply chain services, and wholesale distribution services.

The directive aims to reinforce EU resilience against cyberattacks, crime, public health risks, and natural disasters. It complements the NIS 2 Directive, focusing on cybersecurity measures, both of which entered into force to safeguard critical and digital infrastructures.

eIDAS Regulation

The eIDAS Regulation (Regulation (EU) No 910/2014)¹² establishes a legal framework for electronic identification (eID) and trust services within the European Union. Its primary objectives are to:

- Ensure mutual recognition of electronic IDs across EU member states for secure cross-border transactions.
- Create a standardized and secure environment for trust services, such as electronic signatures, seals, timestamps, and certified delivery.
- Promote interoperability of national eID systems to foster a cohesive digital ecosystem in the EU.
- Enhance trust and security in online services and e-commerce, supporting the digital single market.

11. [Critical entities' resilience](#). July 2023.

12. [eIDAS Regulation](#)

GDPR

The **General Data Protection Regulation (GDPR)** is a European law with large consequences for cybersecurity. European regulations automatically become part of the legislation of all the EU member countries. The GDPR has been enforced since 2018, regulating the use and protection of personal data of European citizens, particularly in electronic systems. In practice, European companies have strict limitations on the collection and use of personal data and must protect their databases according to GDPR requirements.

The GDPR is complemented, at the Spanish level with the LOPDGDD: Data Protection and Digital Rights Guarantee Law (2018).

Crucially, GDPR forbids the **international transfer of the personal data of European citizens** unless the recipient provides valid assurance of data protection to a level similar to that demanded by the GDPR. Some countries are recognized to provide this level of protection in their legal framework, including Canada and the UK, but not the USA. To transfer personal data from the EU to the USA, a European company must prove that the American company receiving the data provides adequate protection. There used to be an agreement between the USA and the EU, the Privacy Shield, that allowed the transfer of European data to America, but European courts overturned it.

This may represent an obstacle for an American company to market its services in Europe if those services imply working with databases containing personal data. Even if American companies provide all required protection, European clients may be reluctant to trust them.

EU cybersecurity certification framework

This framework¹² addresses the current fragmentation of different security certification schemes within the EU by establishing a common set of rules, technical requirements, standards, and procedures for cybersecurity certification. Within it, there are multiple specific certification schemes, each tailored to different types of ICT products and services. Each specific scheme within this unified framework must define:

- The categories of products and services it covers.
- The cybersecurity requirements, such as standards or technical specifications.
- The type of evaluation, whether it's a self-assessment or conducted by a third party.
- The intended level of assurance (basic, substantial, or high).

12. [The EU cybersecurity certification framework | Shaping Europe's digital future](#)

Certified products are recognized across all EU Member States, facilitating cross-border trade and helping inform consumers of product security features. This voluntary EU-wide scheme certifies various ICT products throughout their lifecycle, including biometric systems, firewalls, detection and response platforms, routers, switches, and specialized software.

Currently, two cybersecurity certification schemes are under development, and another has been adopted under this framework:

- A scheme covering ICT products, called the EU Cybersecurity Certification Scheme on Common Criteria (EUCC), was accepted in January 2024. It is based on an existing international scheme called 'Common Criteria'.
- A second scheme in development, 'EUCS', covers cloud services
- The third one, called 'EU5G', is on 5G networks.

Spanish regulations

The legal regulations impacting cybersecurity in Spain are complex, with several laws regulating different aspects and situations. According to the Spanish Cybersecurity Legal Code, the main laws are the following:¹³

- Law 36/2015, of September 28, 2015, on National Security regulates the key principles and bodies and the functions performed for the defense of National Security.
- Order TIN/3016/2011, of October 28, created the Information and Communications Technology Security Committee of the Ministry of Labor and Immigration.
- Law 9/2014, of May 9, 2014, General Telecommunications Law.
- Law 25/2007, of October 18, on the conservation of data relating to electronic communications and public communications networks.

Spain doesn't have a specific cybersecurity law yet, but the current government plans to pass one during its current term (that began in mid-2023 and has a maximum duration of 4 years), likely during 2024. This law will:

- Define special requirements for cybersecurity suppliers hired for critical roles, likely privileging Spanish and European suppliers.
- Define the responsibilities of all Spanish government organizations and the coordination mechanisms.

13. [BOE.es](https://www.boe.es) - Código de Derecho de la Ciberseguridad

Standards

Cybersecurity regulations, standards and certifications are different in the USA and Spain, as well as the European Union. There are standards whose role in the market is similar to CMMC in America, and a lot of the contents might actually be similar, but that doesn't mean that CMMC expertise would be a competitive advantage in Spain.

ISO standards are well known and respected by the market, particularly ISO 27001 and ISO 27032. The European and Spanish standards integrate elements taken from the ISO, while adding more in-depth details.

The EU has approved the EU Cybersecurity Certification Framework (see above).

The Spanish state has approved the **National Security Scheme** (*ENS, Esquema Nacional de Seguridad*). This is a standard that all companies that exchange data with the Spanish administration have to comply with: in this aspect, **its role is similar to CMMC**. Unlike GDPR and Data Protection law, ENS defines technical and organizational measures¹⁴ that companies need to implement if they want to comply with the standard.

The ENS is a relatively recent standard. So far, there are few certification bodies and few companies comply with the ENS.

Generally speaking, cybersecurity certification is an expensive project and most SMEs don't demand certificates, just different cybersecurity tools.

The government has established a National Cybersecurity Strategy, whose last version was approved in 2019.¹⁵ This strategy emphasizes prevention, defense, detection, analysis, response, recovery, and coordination against cyber threats. This comprehensive plan encompasses various sectors, including public administrations, critical infrastructure, military and defense capabilities, cyber-terrorism, cyberspying, cyber-crime, cybersecurity in the private sector, and the promotion of a cybersecurity culture. It fosters public-private partnerships and investing in research initiatives like the Horizon Europe Cluster 3 program. Spanish defense companies like Indra and Navantia are leading efforts in developing advanced cybersecurity solutions for critical infrastructure and military systems.

14. ENS measures (in Spanish): <https://www.ccn-cert.cni.es/publico/ens/ens/index.html#11071>

15. [Estrategia Nacional de Ciberseguridad 2019 | DSN](#)

07. STATUS OF CYBERSECURITY IN KEY SECTORS

Financial Sector

Cybersecurity in the Spanish financial sector:

According to sector sources, **Spanish banks depend on large IT integrators for their cybersecurity activities.** Banks have their own security departments, led by a CISO, but the design and implementation of the systems is generally completed by a systems integrator in the form of a turnkey project. This means that, even if the bank is interested in a specific cybersecurity service or supplier, its point of contact may be the IT integrator.

Some Spanish banks and insurers are very active in the fintech field: for example, managing and financing company incubators and accelerators, investing in startups or running startup competitions and prizes. Some examples include Banco Santander Innoventures, Banco Sabadell Innocells, BBVA Open Talent, Mapfre Insur Space, and Caixa Fintech Zone2Boost. These programs accept both Spanish and foreign startups and may allow the startups to collaborate directly with the bank or even build their services within the bank.

TIBER-ES:

In late 2021, the Spanish Central Bank (*Banco de España*) approved TIBER-ES, a national cybersecurity testing framework. **All financial institutions in Spain can request a TIBER-ES test to assess their cybersecurity.**

In a TIBER-ES test, the simulated attack is performed by a *red-team provider*, usually a third-party specialist company. The EU has published a procurement guide to hire these companies.

TIBER-ES is based on the Threat Led Penetration Testing (TLPT) framework created by the European Central Bank (TIBER-EU). It simulates real cyberattacks to assess and improve cybersecurity defenses. By mimicking the tactics, techniques, and procedures of sophisticated attackers, these tests help institutions prepare for actual cyber threats. Even though any financial institution or market infrastructure operating in Spain voluntarily may decide to undergo a TIBER-ES test, the sophistication of these tests makes them advisable only for institutions that have achieved a certain level of maturity in cyber resilience.

¹⁶ TIBER - ES - Regulations, guidelines and recommendations - Supervised entities

PSD2: Payment Services Directive (PSD)

The Payment Services Directive is the current European Union regulation on payment services and payment providers with extremely important security requirements for banks and online banking. An initial version was adopted in 2007, and the current one in 2015.

Notably, the directive contains strong customer authentication (SCA) requirements for most electronic payments, mandating multi-factor authentication. Authentication must be based on the use of three types of independent elements: knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is). The PSD requires the use of at least two elements but recommends three.

In practice, these elements include the user's mobile phone, a physical token, a software token, a PIN, a password, fingerprints, face recognition, etc. Many companies in the European market offer services to banks related to one or several of these authentication methods.

DORA: Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA)¹⁷ is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025. It aims to strengthen the information and communication technology (ICT) security of financial entities and make sure that the financial sector in Europe can stay resilient in the event of severe operational digital disruption. DORA harmonizes the rules on digital operational resilience for the financial sector, applying to 21 different types of financial entities.

Financial sandbox

A very important opportunity for the development of cybersecurity in the Spanish financial sector is the financial regulatory sandbox that Spain launched in 2020, making it one of the few European countries (seven, at the time of writing) with such a mechanism.

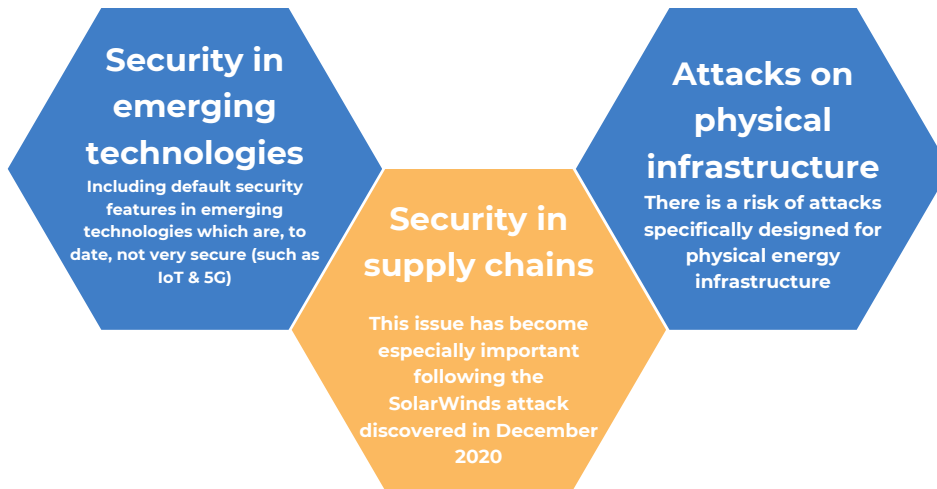
The sandbox is an environment in which financial companies can safely experiment with disruptive technologies and new services while being submitted to a testing protocol and supervision by the authorities. These projects can extend beyond what is allowed or mandated by current regulations, and eventually, laws could be changed to allow successful projects to be marketed to the general public.

The first call for proposals ended in early 2021; 67 projects were submitted and will be approved or rejected by the authorities later in the year. Many projects involve cybersecurity innovations, like using biometrics and other experimental methods for identification.

17. [Digital Operational Resilience Act \(DORA\)](#)

Energy

According to sector sources, the following are a few of the main cybersecurity concerns for the energy sector:



The Spanish government has a specific plan for the cyber protection of critical infrastructure, which includes energy infrastructure (along with transport, healthcare, water, finance, etc.). Operators have special support from the government, through INCIBE, including multiple exercises, attack simulations, audits, and special monitoring. In 2020, INCIBE detected 1,190 attacks on strategic and critical operators.

The most frequent attacks on critical infrastructures in Spain are the following:¹⁸



Incidents in 2020 included a ransomware attack on the electric utility company Endesa. In 2017, the WannaCry attack affected other companies like Gas Natural and Iberdrola.

A 2023 report¹⁹ reveals that 84% of energy companies are prioritizing cybersecurity in their operational technology (OT) environments. The energy sector leads in advancing OT cybersecurity compared to the industry and consumer sectors, where only 46% plan to enhance OT cybersecurity in the next two years.

¹⁸ Avances de España en la protección de sus infraestructuras críticas, January 2021.

¹⁹ El 84% de las energéticas ya avanzan en la ciberseguridad en entornos de producción, según SIA (Indra), November 2023.

The energy sector's progress is driven by stringent regulations for critical infrastructure, despite challenges like a lack of strategic investment and talent shortages. Notably, 68% of energy companies have the necessary professionals for these efforts.

Energy companies need to improve cyber-response capabilities, prediction, automation, orchestration techniques, and increase penetration testing and physical access protection, as 85% lack advanced measures. In contrast, the industry and consumer sectors lag, with only 24% having awareness programs and 23% using advanced OT protection tools. Cybersecurity in operational environments is a strategic priority due to the high exposure and potential impact of attacks, requiring continuous investment to stay ahead of threats. The report's findings are based on interviews with executives and experts from various sectors.

Health sector

A significant cybersecurity breach at Hospital Clínic de Barcelona in March 2023 highlighted the vulnerability of Spain's healthcare system. The attack, claimed by the Ransom House group, disrupted numerous services, including surgeries, lab tests, and radiotherapy sessions. It resulted in the theft of approximately 4 terabytes of sensitive data and a ransom demand of €4.2 million, which was not paid. The healthcare sector suffers from insufficient investment and outdated technology, making it a prime target for cyberattacks. These attacks cost the sector significantly, with an average incident costing around \$1 million.

Impact of the Cyberattack:

- Postponement of over 300 surgeries.
- More than 4,000 lab tests were lost.
- 11,000 outpatient visits missed.

The healthcare sector is highly targeted by cybercriminals, accounting for 8% of cybersecurity incidents from June 2022 to July 2023, according to [ENISA](#). This is behind public administration (19%) but ahead of sectors like banking (6%), transportation (6%), and energy (4%). Health data is highly valuable on the black market, with medical records fetching \$30 to \$1,000 each, compared to \$1 to \$6 for credit card information.

Main threats:

1. Security Misconfigurations (68%)
2. Insider Threats/Human Errors (16%)
3. Social Engineering/Phishing (4%)
4. Supply Chain Attacks, often due to unpatched software or hardware vulnerabilities and the introduction of malware.

Victims:

1. Healthcare Centers (53%) including hospitals (42%).
2. Public Health Authorities (14%)
3. Pharmaceutical Industry (9%)
4. Primary Care (4.5%)

Types of Attacks:

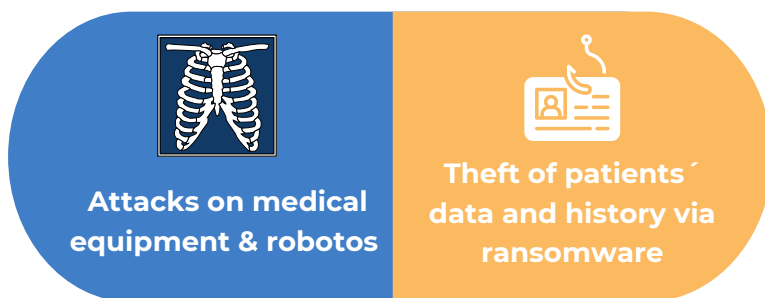
1. Ransomware (54%)
2. Data Theft (46%)
3. Intrusion Attacks (13%)

Targeted Assets:

1. Patient Medical Data (30%)
2. IT Infrastructure Data (28%)
3. Corporate Data (15%)

According to sector sources, healthcare is a highly-specific sector, with needs more similar to the IoT sector than to the IT or industrial sectors. This means that it needs tailored services. The biggest risks in healthcare involve attacks on medical equipment and medical robots and attempts to steal patients' medical data and history²⁰ through the use of ransomware.

Main cyber risks in the healthcare sector



20. [Ciberataques al sistema sanitario en la segunda oleada de la COVID-19](#). February 2021.

As in other countries, the **COVID crisis** caused an increase in cyberattacks against hospitals, especially ransomware. Due to the challenges faced by the health sector in 2020, including its strained capacity and overwhelming workload, when faced with cyberattacks, hospitals often paid ransom to keep their systems running in moments of critical demand. According to CheckPoint Research, attacks against Spanish health companies doubled in 2020.²¹

This has happened even as cybersecurity awareness in the healthcare sector has grown rapidly. According to Hiscox Cyber Readiness Report 2020,²² the cybersecurity-related knowledge and investment of a representative sample of Spanish healthcare companies increased greatly in 2020. However, the general level of cybersecurity preparedness is still low, even when compared to other Spanish sectors.

Until recently, the **Spanish health system's attitude has been reactive and defensive, increasing investment in cybersecurity only when public opinion demands it. The sector does not invest** in hiring internal teams of cybersecurity experts, preferring to outsource the activity instead: external human resources surpass internal ones, with the Ministry of Health reaching a 93% outsourcing rate.²³

In the Spanish administration, most responsibilities over healthcare are decentralized and belong to the regional governments (called autonomous communities – Comunidades Autónomas), which have a higher level of autonomy than in more centralized countries. That's why cybersecurity differs greatly between the **regional healthcare** systems.²⁴ In some regions, cybersecurity is a high priority and is managed by high-ranking employees, while other regions devote fewer resources to it. While there are interregional, collaborative groups that share information and warn about threats, their organizational and budget models are very different.

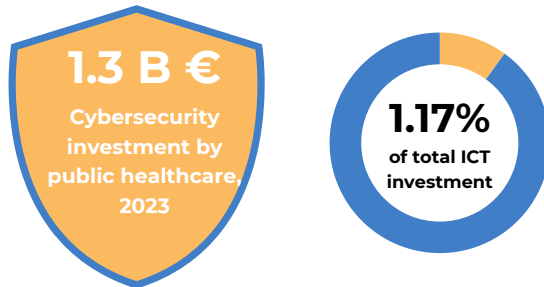
21. [Las empresas españolas del sector salud sufren el doble de ciberataques](#). January 2021.

22. [La industria española de Pharma y Salud aumenta su nivel de ciberpreparación en 2020](#). December 2020.

23. [La inversión TIC de la sanidad pública española crece un 30,87% en 2023](#). AECConsultoras. March 2024

24. ["La ciberseguridad es una inversión, manejamos datos sensibles de los ciudadanos"](#). November 2020.

In 2023, the global ICT investment of Spain's National Health System (SNS) increased by 30.87% compared to 2022, reaching a total of 1.336 billion euros. The overall healthcare budget is 75.743 billion euros,²⁵ with the ICT budget representing 1.17% of this total.



To enter the market, sector sources²⁶ recommend having local partners and having third-party evaluations of the technology to be offered. Sources add, however, that the client base and crisis experience are also vital factors.

Main threats in the health sector

Based on published reference studies (European Union Agency for Cybersecurity 2023);²⁷ it is identified that the most frequent attack vectors, or entry doors in the health sector are:

- Poor security configuration (68%).
- Insiders / human errors in the operation (16%).
- Social engineering/phishing (4%) as an entry vector for intrusion and data theft.

Attacks in the supply chain are also relevant, motivated by unpatched software or hardware vulnerabilities, as well as the downloading and installation of malware or malicious programs within the technological infrastructure.

Regarding the most frequent types of attacks in the healthcare sector, there are:

- Ransomware reaches 54% of the recorded incidents. It is the type of attack with the greatest impact in 43% of cases.
 - Most used ransomware families are: Lockbit, Vice Society and LV group, BackCat /ALPHV.
- Data theft present in 46%.
- Intrusion attacks in 13% of recorded incidents.

25. [Indice 2023 - SEIS](#)

26. ["Una brecha en nuestro ámbito compromete la seguridad \(la salud\) del paciente y su privacidad"](#). December 2019.

27. [Health Threat Landscape – ENISA](#)

Military and defense

The Spanish military has a Joint Cyberspace Command²⁸ that coordinates cybersecurity preparation and response for the three branches of the military. In 2021, the Joint Command intercepted more than 600 potentially dangerous cyberattacks against Spanish military systems. This organization participates in international exercises, like NATO's Locked Shields.²⁹

This command has a staff of approximately 230 military and 50 civilians. It suffers a serious problem of staff rotation, and its leaders consider that it should at least become twice as big to face adequately the probable attacks.³⁰ That's why the military is studying different options to reform and reinforce this command, although no definite decisions have been taken.³¹

The Ministry of Defense has established a Military School of Cyber Operations (EMCO) to train military personnel in cyber defense, reflecting the increasing importance placed on cybersecurity by the Armed Forces in Spain and worldwide. This new institution, under the oversight of the Estado Mayor de la Defensa, aims to provide advanced training in cyber operations in response to evolving threats. It will focus on enhancing the capabilities of the Armed Forces in cyber defense, aligning with national and international cybersecurity strategies. The first 15 specialists graduated in 2024.

28. [Joint Cyberspace Command MCCE](#), Ministry of Defense.

29. [Locked Shields 2024 demonstrated the real power of cooperative defence](#).

30. [El Mando Conjunto del Ciberespacio ha contenido más de 600 ataques peligrosos para la defensa de España en el último año](#), January 2022

31. [Defensa estudia crear un cuerpo propio de militares expertos en ciberdefensa](#), September 2021

06. MAJOR PLAYERS

Largest clients in each private sector

Finance

After the 2008 crisis, the Spanish **banking** sector was dominated by a small number of banks that consolidated and absorbed other institutions.

The two largest banks in Spain are also multinationals with an important foreign presence - Santander and BBVA. Quite a way behind, there are three big, though noticeably smaller banks: CaixaBank, Bankia and Sabadell. These five leaders concentrate 69% of the banking sector's assets.³² This is the highest concentration of all the major European countries.

The rest of the market is formed by much smaller banks: in order of size, these are Bankinter, Unicaja, Abanca, Kutxabank, Ibercaja, and Liberbank. Some of these are descendants of local and regional savings banks, and their presence is geographically limited.

Further fusions are expected: CaixaBank and Bankia (the 3rd and 4th largest) began their merger in March of 2021, while Unicaja and Liberbank (6th and 10th) have approved theirs.

The **insurance** market is also becoming more highly-concentrated, although not to the same degree as the banking market. The leading companies are a mix of Spanish and multinational insurers. The following is a list of the ten biggest insurers:

- | | | | | | |
|---|---|---|--|----|---|
| 1 | VidaCaixa  | 5 | Catalana Occidente  | 9 | Generali  |
| 2 | Mapfre  | 6 | Zurich  | 10 | Santander Seguros  |
| 3 | Mutua Madrileña  | 7 | Axa  | | |
| 4 | Allianz  | 8 | Santalucía  | | |

32. Los cinco grandes bancos ya copan el 70% del mercado con menos competencia. June 2019.

Energy

In Spain, there is a single state company that manages the distribution of electricity (Red Eléctrica de España) and multiple private companies that are in charge of power generation. There are many generation plants using both renewable and non-renewable technologies. The leaders of the electric market are as follows:



These four companies sell 68% of the electricity in the domestic market.³³ Other companies include Fortia, Acciona, Engie, Repsol and Aldro. Recently, the French group Total acquired EDP assets and became an important player.

Red Eléctrica de España has investments in external cybersecurity companies.

Health

In Spain, there are important regional differences in healthcare for two main reasons:

- The 17 regional governments, rather than the national government, are responsible for public hospitals. Each has different policies, and there is minimal coordination between them.
- Spanish regions are very different in terms of size, population, aging, geographic distribution, and, to some extent, wealth.

These differences explain the great disparity between hospitals in different regions of Spain, as well as the variations in the implementation of technological solutions.

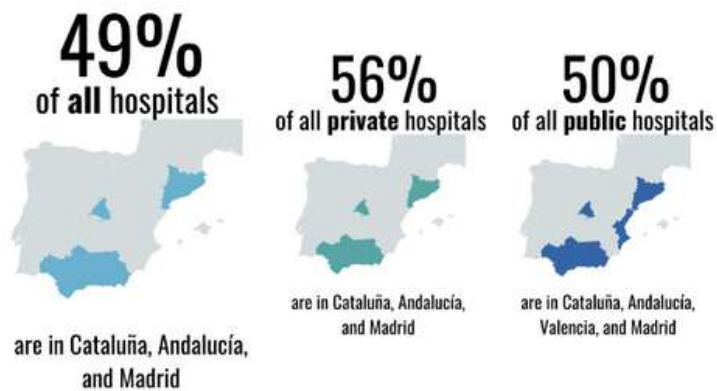
There are 924 hospital facilities in total (Ministry of Health, 2019) - 454 (49%) of which are private, and 470 (51%) of which are public. Between them, there are 158,733 hospital beds.

The regions with a greater percentage of private hospitals compared to public hospitals are Cataluña, Asturias, Navarra, País Vasco, Madrid, Baleares, and Murcia.









33. [La CNMC analiza en un informe el mercado eléctrico en España en 2019](#). January 2021.




The regions with a greater percentage of private hospitals compared to public hospitals are Cataluña, Asturias, Navarra, País Vasco, Madrid, Baleares, and Murcia.

The following regions have the most hospitals (listed from highest to lowest):



In the private sector, the four largest groups are a great deal larger than the remaining companies, which, in general, are fairly small in size. The following table lists the key actors in the private sector:

Group	Number of Hospitals	
Quirónsalud	50	
Vithas	19	
Grupo HLA	15	
HM Hospitales	14	
Hospiten	11	
Viamed Salud	11	
Hestia Alliance	9	
Pascual Hospitales	8	

Group	Number of Hospitals	
Sanitas	4	
Ribera Salud	4	
Clínica Universidad de Navarra	2	

Source: Prepared by the authors with data from each company

It is also important to mention the importance of non-profit institutions belonging to the Catholic Church in the private sector.

Main IT integrators and MSPs

The IT consultant Penteo assessed the Spanish cybersecurity market, identifying 12 companies as market leaders.³⁴ These include a mixture of business consultancy firms, IT consultancy firms, and cybersecurity specialists, both Spanish and foreign multinationals. These market leaders are: Accenture, Ackcent, Eviden, Capgemini, Deloitte, EY, Fujitsu, IBM, Inetum, Minsait-SIA, T-Systems and Telefónica. In other years, they included other companies like S21SEC.

Accenture

<https://www.accenture.com>

<https://www.linkedin.com/company/accenture-espana/>



More than 11,000 workers in Spain across all business lines

IT consultant and integrator. One of the companies with the most extensive cybersecurity experience in Spain, it covers all areas of cybersecurity and has absorbed small, more specialized companies to broaden its offering.

It has cybersecurity technology centers in Madrid and Bilbao.

Accenture offers a range of cybersecurity services and solutions, including Cyber Defense, Identity and Access Management, Application Security, Cloud Security, Data Protection, Cybersecurity Strategy and Risk, Managed Security Services, Security Consulting, Incident Response, and Threat Intelligence, among others

34. [Los proveedores de ciberseguridad más relevantes del mercado español | Computing](#). May 2023.

CAPGEMINI

<https://www.capgemini.com>

<https://www.linkedin.com/company/capgemini/>



More than 5,000 workers in Spain across all business lines.

Capgemini has developed a complete portfolio of tailored services in cybersecurity, a field that has grown within the company, particularly after the acquisition of Altran.

Capgemini offers a range of services including Consulting, Technology Services, Digital Transformation, Engineering Services, Business Services, Cloud Services, Cybersecurity, and Artificial Intelligence and Analytics, among others.

Eviden (Atos group)

<https://eviden.com>

<https://www.linkedin.com/company/eviden/>



Eviden, part of the Atos Group, is a French company with an annual revenue of approximately €5 billion. It offers a wide range of services, including Advanced Computing, Cloud, Digital Security, Generative AI, Sustainability, Smart Platforms, and Transformation Acceleration.

In Spain, Eviden has an office located in Madrid. The company serves various sectors, such as Energy & Utilities, Healthcare & Life Sciences, Financial Services & Insurance, Manufacturing, Public Sector & Defense, Retail, Transport & Logistics, and Telecom, Media & Technology.

Deloitte

<https://www2.deloitte.com>

<https://www.linkedin.com/company/deloitte-espana/>



A leader in the Spanish market with a complete and diverse portfolio of cybersecurity services, including Cyber Strategy, Risk Management, Threat Intelligence, Incident Response, Identity and Access Management, Data Protection, Cloud Security, Application Security, and Managed Security Services.

In Spain, it has centers in Madrid and Barcelona. Its Madrid SOC, launched in 2013, was one of the first global SOCs for the company.

It has notable clients in banking and the public sector; in December 2020, Deloitte won a public tender to manage the cybersecurity of the Spanish central bank.

EY

https://www.ey.com/es_es

<https://www.linkedin.com/company/ernstandyoung/>



The company has invested heavily in cybersecurity, with significant growth in recent years. It has two local operations laboratories with incident detection and response, identity management, data protection and resiliency services. It is ISO 27001 certified. The company has 4,700 workers in Spain across all its business and service lines.

EY offers a full range of services including Cybersecurity Strategy, Risk, Compliance and Resilience, Data Protection & Privacy, and Cyber architecture, operational technology and engineering services, among others.

Google

<https://abc.xyz>

<https://www.linkedin.com/company/google>



Google has launched its Google Safety Engineering Center (GSEC) in Málaga (over 650 M USD), Spain, aiming to enhance cybersecurity across Europe. This new center is one of only three in the world, with the other two located in Dublin and Munich. Google chose Málaga due to its vibrant tech ecosystem and its acquisition of the local cybersecurity firm VirusTotal in 2012.

Google announced a €9.1 million investment to boost cybersecurity training and support local NGOs, addressing the chronic shortage of cybersecurity talent in Europe, which requires 500,000 professionals. The center will collaborate with various entities to advance cybersecurity knowledge and practices. The center aims to protect sectors such as healthcare, finance, and communications, which rely heavily on interconnected networks. The center will include a dedicated training area that will host customized workshops for government officials, businesses of all sizes, job seekers, NGOs, and local schools.

IBM

<https://www.ibm.com>

<https://www.linkedin.com/company/ibm/>



More than 2,500 workers.

IBM has a diversified cybersecurity portfolio, including products and end-to-end services with automation capabilities, managed services, and monitoring. Its clients in Spain include some of the country's biggest companies, like the bank BBVA.

35. [New cybersecurity center in Málaga will help build a safer Europe](#). November 2023

ICA Sistemas

www.grupoica.com

<https://www.linkedin.com/company/grupo-ica>



One of the leading cybersecurity suppliers to the government, alongside banks and utilities.

ICA Sistemas is a Spanish company headquartered in Madrid, with regional offices in Barcelona, Seville, Cadiz, and Huelva. With 670 employees and over 35 years of experience, they specialize in Digital Transformation, Cybersecurity, Communications Infrastructure, and IT Professional Services. They provide tailored hardware, software, and service solutions to meet the specific needs of both public and private entities.

INDRA-SIA

<https://www.sia.es/>

<https://www.linkedin.com/company/sia-group>



Indra is the largest IT integrator in the Spanish market, with over 35,000 workers, and a frequent partner and supplier to the largest Spanish companies in every sector, including the public sector: the Spanish government holds 18% of its capital.

SIA (Sistemas Informáticos Abiertos) is an Indra subsidiary since 2020, and it is an important cybersecurity specialist, with 1,800 workers and a comprehensive range of cybersecurity services.

The Indra-SIA merger positions the consolidated company as a benchmark in the Spanish cybersecurity market. At the Spanish level, it is one of the largest providers of both talent and solutions in cyberdefense.

NTT Spain

<https://es.nttdata.com/>

<https://www.linkedin.com/company/ntt-data-europe-latam/>



NTT Spain is one of the leading companies in public tenders for cybersecurity.

NTT Data, originating from Japan, operates extensively across Spain with a total of 18 offices. Its main Spanish headquarters is located in Madrid. The company specializes in providing a wide range of services within the ICT sector, including consulting, application, business process, cloud, and infrastructure services.

NTT Data caters to various industries such as Banking, Infrastructure, Services & Real Estate, Retail, Consumer Goods, Insurance, Telecom & Media, Energy and Utilities, Manufacturing & Automotive, Travel, Transportation & Logistics, Healthcare, Public Sector, and Green Deal & Sustainable Engineering.



NUNSYS

<https://www.nunsys.com/>

<https://www.linkedin.com/company/nunsys>

NUNSYS is one of the leading companies in public tenders for cybersecurity.

NUNSYS is a company specializing in the implementation of integral technology solutions across Spain. They focus on projects in the field of communications, systems, networking, and software for both private companies and public entities. NUNSYS operates with 15 offices located throughout Spain, with its main headquarters based in Valencia.

Solutia

<https://gruposolutia.com/>

<https://www.linkedin.com/company/solutia-innovaworld-technologies>



Solutia is one of the leading companies in public tenders for cybersecurity.

Grupo Solutia is a Spanish ICT company based in Seville, with offices in both Madrid and Seville. Their services include solutions for the workplace, data center solutions, application development and management, eHealth, cloud solutions, audiovisual solutions, networking, ICT classroom solutions, outsourcing services, and ECM/document management.

They serve diverse sectors such as public administration, commerce, hospitality, catering, health, medicine, biology, environment and water management, education, transport, distribution, engineering, technology, telecommunications, industry, manufacturing, marketing, communication, and events.

Telefónica Cybersecurity & Cloud Tech - ElevenPaths

<https://www.elevenpaths.com>

<https://www.linkedin.com/company/eleven-paths/>



Telefónica is the leading telecommunications operator in Spain and one of the largest in the world, with operations in Europe, America and Asia. Telefónica has a security division, Telefónica Cybersecurity & Cloud Tech, and its cybersecurity subdivision is known by the brand name ElevenPaths.

Telefónica promotes startups through its own accelerator (Wayra) and direct investment (Telefónica Tech Ventures), with a special focus on cybersecurity, and it has acquired several startups. Telefónica's cybersecurity services have grown considerably, partly through these acquisitions, with approximately 2,500 workers in the subsidiary and a revenue of 497 million euros in 2019.

Telefónica is both a developer of its own cybersecurity products and a distributor of third parties' products. It has tailored solutions for the manufacturing, banking, and public sectors, among others. Its most important clients include energy companies and banks.

Leading cybersecurity specialists and MSSPs

ACKCENT

<https://ackcent.com>

<https://es.linkedin.com/company/ackcent>



More than 50 workers.

Ackcent is focused exclusively on offering cybersecurity services and solutions, with a comprehensive portfolio such as Incident Response Management Programs, Automation and Orchestration, Intelligence Operations, Cybersecurity Architecture and Implementation, among others. Its headquarters are in Barcelona, with branches in Madrid, Zaragoza, the United Kingdom, and Mexico. It has relevant clients in banking, insurance, and the public administration, in addition to other sectors.

To further enhance their services, they partner with companies such as SentinelOne, Sumo Logic, Palo Alto, Imperva, IntSights, Qualys, Checkmarx, and Ironscales.

Entelgy (Innotec)

<https://innotec.security>

<https://es.linkedin.com/company/entelgy-innotec-security>



350 employees.

This company specializes in cybersecurity, with an advanced security operations center (SmartSOC) which was opened a few years ago. Entelgy collaborates regularly with public organizations as well as with 250 other large companies in Spain and Latin America. The company was acquired by Accenture in November 2023 but continues to operate independently.

Innotec Security offers a range of services and solutions, including Pentesting, Tiber Exercises, IT/OT Risk Management, Digital Risk Protection, Detection & Response, and overall Infrastructure Security, among others.

MTP

<https://www.mtp.es/>

<https://www.linkedin.com/company/mtp-metodos-y-tecnologia/>



It is one of the leading companies in public tenders for cybersecurity.

MTP Métodos y Tecnología is a consulting firm headquartered in Madrid, Spain, with 3 other offices across the country and a team of over 1000 employees. Specializing in Software Quality Assurance services, they focus on optimizing software product lifecycles and construction processes for industries such as Telecommunications, Banking, Insurance, Utilities, and Public Administration.

Panda Security

<https://www.pandasecurity.com/>
<http://www.linkedin.com/company/panda-security>



More than 500 workers

Developers of one of the best known antivirus software, they also provide cybersecurity outsourcing to businesses and governments. The company was acquired by WatchGuard Technologies in 2020 but continues to operate independently. They have partnerships with companies such as Deloitte, StormShield, Vector ITC Group, and Masscomm in Spain.

S2 Grupo

<https://s2grupo.es>
<https://www.linkedin.com/company/s2grupo/>



400 workers.

Cybersecurity specialists in three main sectors: IT, industrial OT, and healthcare. They offer cybersecurity, cyber-intelligence, and mission-critical system operations. S2 has Security Operations Centers in Valencia, Madrid, Mexico City, and Bogotá.

They have partnerships with Mundo R, Blu5, Euskaltel, and Andersen to enhance their services in the Spanish market and ensure compliance with Spanish data security laws and regulations.

S21SEC

www.s21sec.com
<https://es.linkedin.com/company/s21sec>



More than 500 workers

S21sec is one of the oldest cybersecurity specialists in Spain. It is a software developer, distributor, and integrator that provides services to various sectors, including healthcare, energy, finance, and public administration. Its service portfolio is comprehensive, covering all aspects of cybersecurity.

Currently, S21sec plays an important role in the market, especially after the company was purchased by the Portuguese Sonae IM fund (part of the Sonae group, one of the largest holding companies in Portugal) and its subsequent merger with Nextel. Sonae IM is expanding its cybersecurity business with acquisitions in other European countries, like Belgium, and building one of the largest cybersecurity pure players in Europe, with more than 500 workers thus far.

In 2020, S21sec worked closely with healthcare clients to guarantee their security during the COVID crisis. The company was acquired by Thales in 2022 but continues to operate independently.

Trend Micro

<https://www.trendmicro.com>

<https://es.linkedin.com/company/trend-micro-europe>



US multinational company that has become one of the main players in Spain and Portugal. Trend Micro Europe offers a range of cybersecurity services and solutions, including Endpoint, Network, Email, and Cloud Security, Threat Intelligence, Data Protection, and Security for IoT, among others.

With headquarters in Madrid, they partner with other cybersecurity companies such as IBM, BeDisruptive, LogRhythm, and MNEMO to further enhance their reach and services in the Spanish market.

Other companies

There are many other companies, both large and small, in the Spanish cybersecurity market. A list is provided as an annex.

Some smaller ICT integrators offering cybersecurity solutions include the following:

Company	Website	Description
Axians	www.axians.es	High penetration in the public sector
Delaware	www.delawareconsulting.com	Solutions for energy and healthcare, among others
everis	www.everis.com	Hospital software and high penetration in the public sector
GMV	www.gmv.com	Services for banking, insurance, public administration and healthcare
Ibermática	www.ibermatica.com	Offers services to a range of sectors, including healthcare, energy, finance and public administration
SEIDOR	www.seidor.es	High penetration in the public sector
SIRT	www.sirt.com	Presence in banking, public administration, healthcare, and other sectors
TAISA	www.taisa.com	High penetration in the public sector, utilities, and finance

Public institutions

INCIBE

<https://www.incibe.es>

INCIBE is the Spanish government's cybersecurity authority. It is an agency within the Ministry for the Economy and Digital Transformation. INCIBE works for the public administration, citizens, and businesses.

INCIBE's tasks include:

- Monitoring of cybersecurity threats and incidents
- Managing the government's Computer Emergency Response Team (CERT or CSIRT)
- Promotion of research
- Promotion of entrepreneurship and cybersecurity startups
- Publications, information, and guides
- Self-diagnostic tools
- Promoting and coordinating cooperation between cybersecurity companies and the public administration
- Offering events, conventions, and seminars
- Training

Its HQ is located in the city of León, in northwestern Spain, two to three hours from Madrid. A cluster of cybersecurity companies has grown there.

It is one of the three government Computer Emergency Response Teams in Spain.

NATO has chosen the INCIBE to be part of its Defence Innovation Accelerator for the North Atlantic (Diana) program, making it one of the twenty-three global centers for defense innovation under this initiative. Incibe will serve as the sole accelerator in Spain for innovative cybersecurity startups, receiving access to funding and support to develop dual-use technologies for both civilian and military purposes. The Diana program aims to foster transatlantic collaboration and technological advancement in defense through accelerators and test centers, with a focus on improving operational deployment, interoperability, and maintaining a technological edge amidst evolving global threats.

INCIBE Emprende



incibe
emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#INCIBEmprende

VEDP

INCIBE is addressing the rising demand for cybersecurity with a new initiative aimed at promoting cybersecurity among entrepreneurs. This event, organized by INCIBE, focuses on supporting entrepreneurs and startups with innovative ideas and projects in cybersecurity. Through this public invitation, INCIBE aims to foster the development of business ideas and the incubation and acceleration of entrepreneurship projects. The event is supported by major IT companies in Spain, such as Telefónica, as well as other private and public entities. The selected startups will receive comprehensive support throughout the entire process, from ideation to incubation and acceleration, ensuring they have the resources and guidance needed to succeed in the cybersecurity sector.

Joint Cyberspace Command (MCCE)

As previously explained, it is a joint department that coordinates cyberspace actions for all three branches of the military. It is another of the three government Computer Emergency Response Teams in Spain.

National Cryptology Center (CCN)

This center provides cybersecurity response against attacks that target the Spanish administration systems. It is the last of the three government Computer Emergency Response Teams in Spain.

Regional cybersecurity authorities

Some regional governments have created cybersecurity centers that support the region’s businesses and citizens.

Center	Website
Catalonia Cybersecurity Agency	https://ciberseguretat.gencat.cat
Basque Cybersecurity Center	https://www.basquecybersecurity.eus
Valencia ICT Security Center	https://www.csirtcv.gva.es/
Galicia CSIRT	https://amtega.xunta.gal/es/csirt

CyberCAT: A cybersecurity cluster that brings together companies, research institutions, and public entities to promote collaboration and innovation in cybersecurity and information privacy within Catalonia, aiming to strengthen its international impact.

- Cybasque: An association that was created with the aim of promoting collaboration between companies, professionals, and stakeholders dedicated to cybersecurity in the Basque Country.
- Centro de Ciberseguridad Industrial: A non-profit association uniting professionals and entities, both private and public, focused on cybersecurity challenges in automation and industrial digitization. The association strengthens industry cybersecurity in Europe and Latin America through relationship-building, knowledge-sharing, and cross-sectoral experience exchange

Spanish Central Bank:

It oversees cybersecurity testing for the Spanish financial sector.

Business Associations

- AEC: Spanish Business Consulting Association. Cybersecurity is an important focus for the association, which includes leading providers such as Indra, Deloitte, CapGemini and Accenture.
- AEFI: Spanish Fintech Association.
- TICBiomed: Services for digital health companies include visibility, matchmaking, search for funding, regulatory support, and business model consulting.
- SEIS: A professional association, although it is sponsored by businesses. It offers activities typically associated with professional associations, such as congresses and training workshops. Spanish Association for the Evaluation of Health Technologies
- FENIN: Spanish Federation of Health Technology Businesses.
- ASPE: National association for the private healthcare industry, including hospitals, clinics, laboratories, specialized logistic providers, etc. Their members include 80% of private hospitals in Spain.
- Clúster de Ciberseguridad de Andalucía: An organization that integrates businesses, associations, and public and private institutions to promote the development of Andalusia's cybersecurity ecosystem.

06. INTERNATIONAL EXPANSION

The **international links** of the Spanish market are one of its most important characteristics. We can highlight two of them: links with the EU, and links with Latin America.

As many parts of this report show, Spain shares a lot of laws, rules, standards and policies with the rest of the **European Union**. Thanks to the European single market, companies that get any kind of authorization required to work in one EU country, can work in all the other EU members. European companies are present in the Spanish cybersecurity market. Research institutions and government administrations collaborate in cross-border European projects, establishing links that help businesses.

With **Latin America**, the link comes from the historical and linguistic connections those countries have with Spain. Due to their shared history and language, Spain has a special relationship with Latin America.

In the economic field, this takes the form of increased flows of goods, people, companies and investment between Spain and Latin America. A certain cultural familiarity and the shared language make establishing business relationships much easier.

Latin American countries are often among the first markets in Spanish businesses' expansion process, both for exports and for subsidiary opening. That's why **Spain is the second largest investor in Latin America after the US** (and the largest European investor). It has a presence in 11 of the 19 countries in the region and although the bulk of the capital is located in Mexico and Brazil, in recent years there has been significant progress in Colombia and Argentina. The Institute of Economic Studies highlights that investments are concentrated in the services branch, with special prevalence in the financial sector (29.2%), telecommunications (10.2%), energy (8.4%) and extraction oil and natural gas (7.7%). It is estimated that in 2023 the total investment from Spain to the region will exceed 153 billion euros, according to the same source.³⁵

The same happens often for Latin American companies that want to enter the European markets. Spain is the second global destination for Latin American investments. Latin America is the fourth largest investor in Spain, preceded by the United States, the United Kingdom, and France, and ahead of European economic partners of importance such as Germany or Italy.

35. [España se afianza como segundo inversor en Latinoamérica | CapitalMadrid](#)

Eleven Paths - Telefónica

Eleven Paths is Telefonica's global cybersecurity unit. In 2020, they announced a strategic collaboration with Chronicle, a cybersecurity solutions company part of Google Cloud, to provide more powerful and flexible managed security analysis services for companies in Europe and Latin America. Among other projects, Telefonica has SOCs in Mexico, Brazil, and Colombia. It has worked for Latin America's fourth-largest oil and gas company, Ecopetrol (Colombia).

S2 Grupo

A Spanish company contributes to strengthening the cyber defense of strategic companies and public administrations in more than 35 countries. Their strategy for Latin American countries focuses on expanding their presence in the region, where they provide services in more than 14 countries. Their non-Spanish SOCs are located in Mexico and Colombia, and the Mexican Senate is one of their clients.

Entelgy

Spanish business-tech consultancy specialized in global transformation accelerators, with a presence in countries such as Argentina, Brazil, Chile, Colombia, México, Peru, and the USA.

One of the greatest success cases in Colombia was with Fiduprevisora, a consumer protection organization. The project involved solutions focused on an OpenShift platform, containerization, contingency registry, stability registry, security protocols, monitoring, etc.

Indra-SIA

SIA is the cybersecurity arm of Indra, the largest IT company in Spain. It has clients in Colombia, Mexico, and Brazil and operations in Panama, Chile, Peru, and El Salvador. Indra opened its first SOC in Mexico in 2015.

Sofistic - Soluciones 480

This is an example of a smaller company, entirely focused on cybersecurity, that has SOCs in Panama, Colombia, Costa Rica and the Dominican Republic. It provides services to the banking sector and critical infrastructures.

INCIBE, the Spanish National Cybersecurity Institute, has, among their functions, promoting the international expansion of the Spanish cybersecurity industry³⁶. For this, INCIBE participates in international events, with a focus on Europe and Latin America, establishes collaboration agreements with Latin American institutions (most recently, with the Mexican ICT Federation), and promotes the presence of Spanish businesses in that area.

36. [Internacionalización de empresas de ciberseguridad | ED2026 | INCIBE](#)

06. TRADE FAIRS AND EVENTS

Cyber Security World

Website: <https://www.cybersecurityworld.es>

Location: Madrid

Next edition: 16-17 October 2024

Description: Although it is a new trade fair for Madrid, it is, in fact, a local edition of an event that already exists in London, Paris, Frankfurt, and Singapore. Goals for 2021 include exceeding 200 exhibitors and 8,000 visitors.

CISO Day

Website: <https://cisoday.es/>

Location: Madrid

Dates: Every year

Next edition: June 26, 2024

Description: CISO Day in Spain is an annual event dedicated to Chief Information Security Officers (CISOs) and cybersecurity professionals. It serves as a platform for discussing the latest trends, challenges, and best practices in the field of information security. The event typically includes keynote speeches, panel discussions, and networking opportunities, bringing together experts, vendors, and organizations to share knowledge and collaborate on improving cybersecurity measures. CISO Day aims to highlight the critical role of CISOs in protecting digital infrastructure and fostering a culture of cybersecurity awareness.

Digital Enterprise Show

Website: <https://www.des-show.com/>

Location: Málaga

Dates: Every year

Next edition: May 13-15, 2025

Description: The Digital Enterprise Show (DES) is a major annual event that focuses on digital transformation and innovation in business. It brings together industry leaders, technology experts, and professionals to explore the latest trends and solutions in digital enterprise, including cybersecurity.

IOT Solutions World Congress

Website: <https://www.iotsworldcongress.com/>

Location: Barcelona

Dates: Every year

Next edition: May 13-15, 2025

Description: The IoT Solutions World Congress focuses on the industrial applications of IoT technology, including cybersecurity. It brings together industry leaders and experts to discuss how IoT is transforming sectors like manufacturing, healthcare, energy, and transportation. The event includes keynote presentations, panel discussions, and workshops, along with an exhibition showcasing the latest IoT and cybersecurity solutions.

SICUR

Website: <https://www.ifema.es/sicur>

Location: Madrid

Dates: Every 2 years

Next edition: Early 2026

Description: SICUR is a multi-sector security fair, with cybersecurity a focus of the event. More than 700 exhibitors and more than 42,000 professional visitors..

ASLAN

Website: <https://aslan.es>

Location: Madrid

Dates: Every year

Next edition: Spring 2025

Description: ASLAN is one of the main IT events in Spain, with 30 previous editions. Cybersecurity is one of its 5 main sectors. More than 125 exhibitors and 7,500 professional visitors.

National Cyberleague

Website: <https://www.nationalcyberleague.es>

Location: Madrid

Dates: Every year

Next edition: October-November 2024.

Description: This event is a cybersecurity hackathon and competition for IT students and cybersecurity staff in the Spanish administration and military.

ENISE (Encuentro Internacional de Seguridad de la Información)

Website: <https://www.incibe.es/eventos/enise>

Location: León

Dates: Every year

Next edition: October 21-23, 2024

Description: **This is the most important event of Cyber in the Spanish speaking economy.** It is a cybersecurity hackathon and competition for IT students and cybersecurity staff in the Spanish administration and military. Organized by the Instituto Nacional de Ciberseguridad (INCIBE) in Spain. It focuses on bringing together cybersecurity professionals, companies, government agencies, and academic institutions to discuss the latest trends, challenges, and solutions in information security.

Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)

Website: <https://www.incibe.es/eventos/JNIC>

Location: Held annually in different cities across Spain

Dates: Every year

Next edition: Summer 2025

Description: Organized annually by an institution selected by INCIBE, this congress serves as a meeting point for various stakeholders in the field of cybersecurity research. Participants include universities, technology and research centers, businesses, and public administration. The event facilitates the exchange of knowledge and experiences with the common goal of advancing cybersecurity research at the national level.

Barcelona Cybersecurity Congress

Website: <https://www.barcelonacybersecuritycongress.com/>

Location: Barcelona

Dates: Every year

Next edition: May 13-15, 2025

Description: This event is focused on addressing the challenges and advancements in cybersecurity. It brings together experts, industry leaders, and professionals from around the world to discuss cybersecurity trends, threats, and solutions. The congress features keynote speeches, panel discussions, workshops, and exhibitions.

Gartner IT Symposium/Xpo

Website: <https://www.des-show.com/>

Location: Barcelona

Dates: Every year

Next edition: November 4-7, 2024

Description: Organized by the American company Gartner, this is a significant event for CIOs and senior IT executives. It focuses on strategic insights, industry trends, and emerging technologies shaping the future of IT and business. Attendees may engage with analysts, industry experts, and peers to explore solutions to critical challenges and gain actionable guidance for their organizations. The event covers a wide range of topics, including cybersecurity, data analytics, and IT strategy.

Osintomático

Website: <https://osintomatico.com/>

Location: Madrid

Dates: Every year

Next Edition: May 2024

Descripton: An event focused on Open Source Intelligence (OSINT) and digital security. Held annually in Madrid, this conference serves as a significant platform for cybersecurity professionals, including members from intelligence agencies such as the CNI (Centro Nacional de Inteligencia). The event features a variety of sessions, workshops, and presentations led by international experts in fields such as social engineering, blockchain, and digital forensics. Participants have the opportunity to enhance their skills and exchange knowledge on the latest trends and techniques in cybersecurity.

Congreso C1b3rWall

Website: <https://c1b3rwall.policia.es/congreso>

Location: Madrid

Dates: Every year

Next edition: June 18-20, 2024

Description: The C1b3rWall Congress is a cybersecurity event held annually in Spain, specifically organized by the National Police, Cuerpo Nacional de Policía (CNP). The congress aims to bring together experts, professionals, academics, and students in the field of cybersecurity to share knowledge, research, and best practices. The event features lectures, workshops, and panel discussions that cover various aspects of cybersecurity such as cybercrime, digital forensics, data protection, and emerging threats.