May 2025. Technological snapshot.

Cybersecurity in Catalonia

Generalitat de Catalunya

Cybersecurity in Catalonia. Technological snapshot.

ACCIÓ
Generalitat de Catalunya

The use of brands and logos in this report is merely informative. The above-mentioned brands and logos belong to their respective owners and are not owned by ACCIÓ in any way. This is a partial illustrative representation of the companies, organizations and entities that are part of the cybersecurity ecosystem. There may be companies, organizations and entities that have not been included in the study.

Carried out by
Strategy and Competitive Intelligence Unit of ACCIÓ
Cybersecurity Agency of Catalonia

Barcelona, May 2025

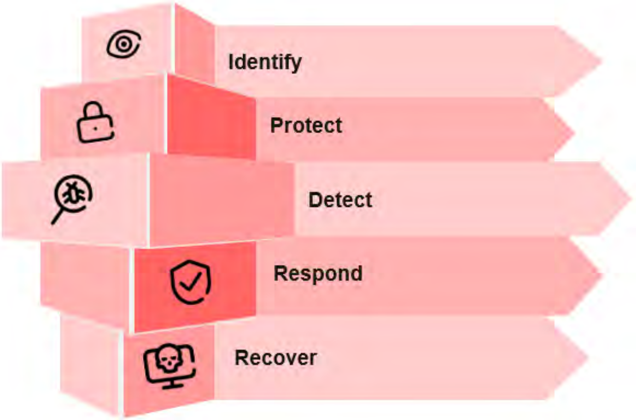
Generalitat
de Catalunya

Contents

Executive summary: cybersecurity in Catalonia (I)

Cybersecurity is the set of physical, logical and governance measures that protect data properties and information systems.

Verticals



Core demand sectors

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT service management (B2B)
- Public Administration
- Space

Impact of quantum technologies

Main opportunities in cybersecurity:

- Quantum security cryptography
- Ultra-secure communication
- Improved threat detection

Global market

The global turnover in cybersecurity will grow at an **annual rate of 8%** over the next five years and reach **$272 B**.

America boasts a prominent lead in the cybersecurity market, while **Europe** and Asia stand in second and third position, respectively.

Financial services, the **public administration** and **health** are the sectors with the highest demand for cybersecurity services.

Over the last five years, cybersecurity-related **FDI** has accumulated investment totaling **€41 B**, while cybersecurity startups have completed **venture capital rounds** worth **$11 B**.

Executive summary: cybersecurity in Catalonia (II)

557 companies in the cybersecurity ecosystem

A **7.9% annual increase** and one of **58.2%** since 2018.

A **€1.473 B** (**+18.4%**) turnover and **10,672** jobs (**+12.8%**).

82.6% are SMEs and **10.6%** are startups.

By segments, we should highlight the companies that **protect** (**90.3%**) and **identify** (**62.5%**).

238 companies (42.7%) also develop solutions with **AI**

27 companies (4.8%) also develop solutions with **quantum**

Catalonia, an attractive region for cybersecurity

FDI projects in cybersecurity in Catalonia have **doubled** over the last five years, while **investment** has multiplied by **9**.

36% of the 160 technological hubs of international companies based in Catalonia focus on cybersecurity.

Catalonia is the **5th-ranked European region** in terms of funding by Horizon Europe (2022-2024), with **15 projects** and **€11.3 M**.

Cybersecurity talent

14 undergraduate, master's and postgraduate degrees in cybersecurity and **62** vocational training courses in cybersecurity.

The talent gap is widening by an annual **12.8%** and it currently stands at **13,500** people.

Initiatives to promote cybersecurity in Catalonia

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA – CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

BARCELONA CYBERSECURITY CONGRESS

CYBER[SECURITY]CAT

DIH4CAT Digital Innovation Hub de Catalunya

DCA Digital Catalonia Alliance

ASCICAT ASSOCIACIÓ DE CIBERSEGURETAT DE CATALUNYA

Initiatives quantum - cybersecurity

- **QSunset**
- **6GQuiCryptoLab**
- **Qspace**
- **Quantum cryptography roadmap**
- **Qollserola**
- **Node Barcelona - Q-Network**

1. Definition of cybersecurity and its importance for industry

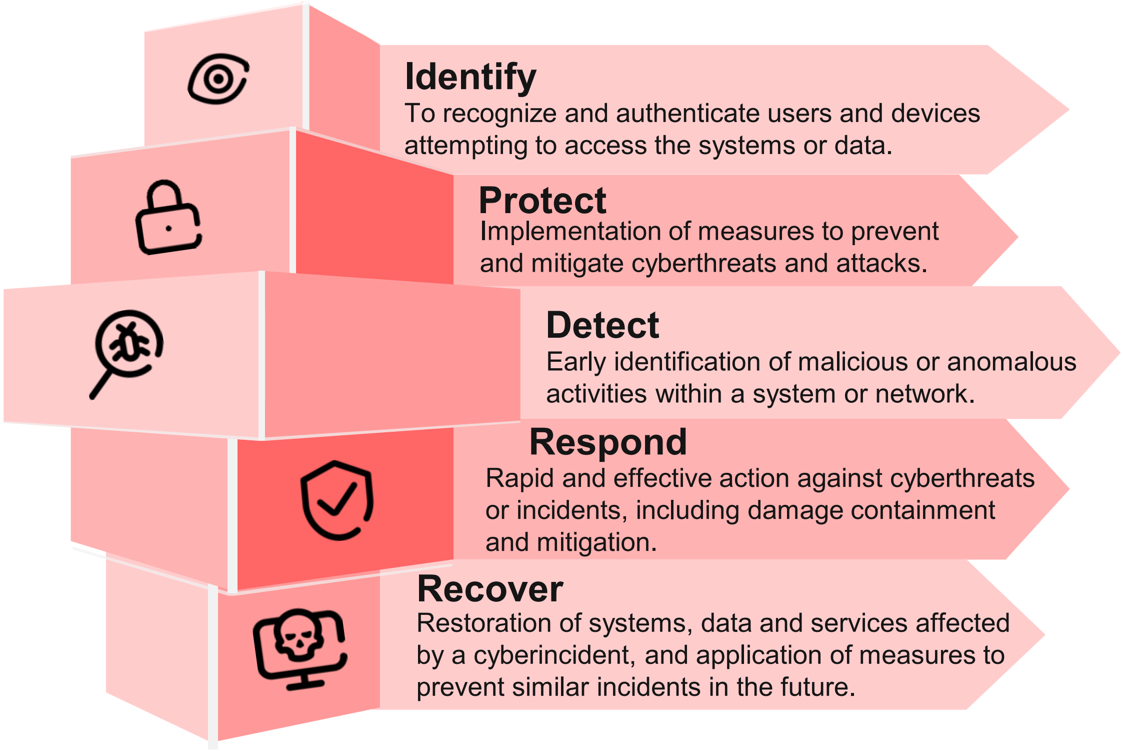
Definition of cybersecurity

Cybersecurity is the set of physical, logical and governance measures that protect data properties and information systems.

The properties of the data and information systems include:

- **Confidentiality:** This guarantees that only authorized persons can access the data.
- **Integrity:** This guarantees that they will not undergo any alteration or voluntary or accidental destruction.
- **Availability:** This guarantees full functioning when the data and system are requested.
- **Authenticity:** This guarantees that an entity is what it claims to be or confirms the source the data come from.
- **Traceability:** This guarantees the possibility of knowing the source, use, route and location.

Cybersecurity consists of **comprehensive and holistic threat management**, ranging from identification and protective measures to the detection of cyberattacks, responses to cyberincidents and recovery.



Identify
To recognize and authenticate users and devices attempting to access the systems or data.

Protect
Implementation of measures to prevent and mitigate cyberthreats and attacks.

Detect
Early identification of malicious or anomalous activities within a system or network.

Respond
Rapid and effective action against cyberthreats or incidents, including damage containment and mitigation.

Recover
Restoration of systems, data and services affected by a cyberincident, and application of measures to prevent similar incidents in the future.

Act on:

People

Processes

Technologies

Magnitude of cybercrimes

In global terms, by 2024 it is estimated that the economic cost of cybercrime activity has stood at around **9.5 trillion euros**.

In 2024, ransomware attacks have increased by a global **11%** with respect to the previous year.

News stories about impersonation fraud have increased by **50%** in 2024 compared to the previous year.

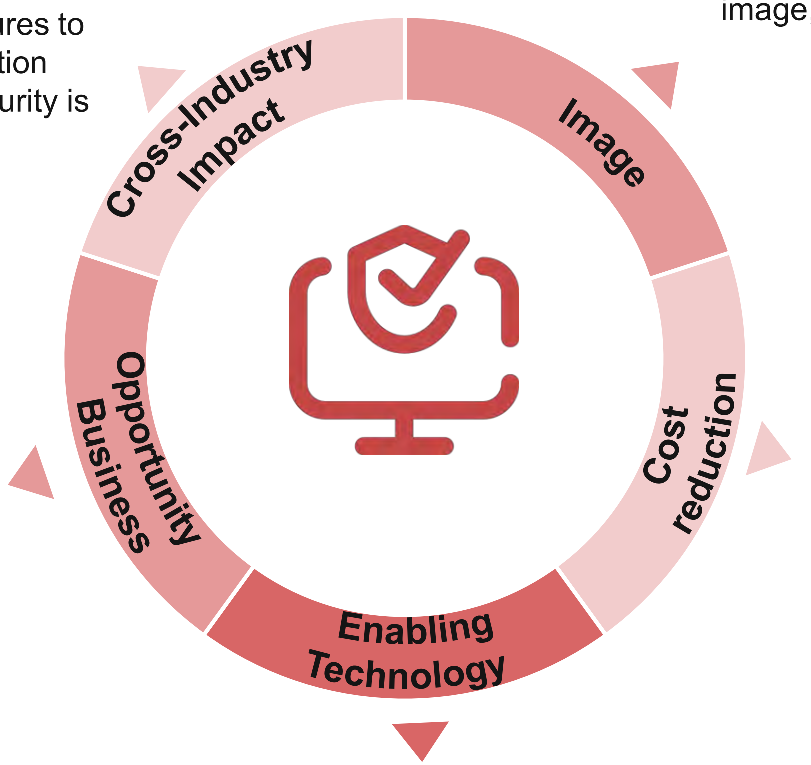
91% of ransomware attacks in 2024 have included data leaks, an increase from 75% in 2023 and 60% in 2022.

Cybercriminals have stolen more than **€2 B** in cryptocurrencies in 2024, an increase of **10%** with respect to the previous year.

In Spain, cybersecurity incidents have risen by **15%** in 2024 compared to the previous year.

Sources: Cybersecurity Agency of Catalonia, INCIBE, RansomDB, Blackfog

Importance of cybersecurity for industry



Cyberattacks are affecting more and more areas, from governments and infrastructures to financial services, smart cities, production processes and health systems. Cybersecurity is essential to protect them.

A cyberattack can significantly affect the company's image, trust and reputation among both customers and investors.

The implementation of good cybersecurity measures to prevent vulnerabilities can lead to cost savings, thanks to the reduction in hours taken up by system shutdowns and restarts, device repair, data leaks that can expose private or sensitive information, data rescue payments and legal repercussions.

Cybersecurity is essential for the full development and hybridization of other innovative technologies, such as artificial intelligence, the Internet of Things and digital twins. Without cybersecurity there is no Industry 4.0, advanced mobility or digital health.

An increasingly connected environment makes it possible to generate new companies that develop technologies for certain types of attacks and new business models based on the vulnerability studies. New opportunities for startups, business transformation and job creation.

Source: the authors

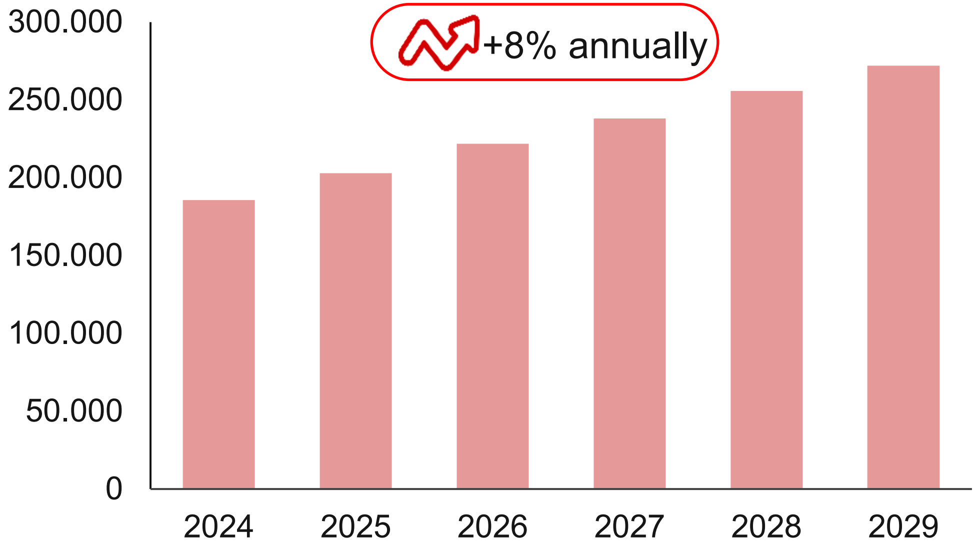
2. Main global magnitudes

The world cybersecurity market

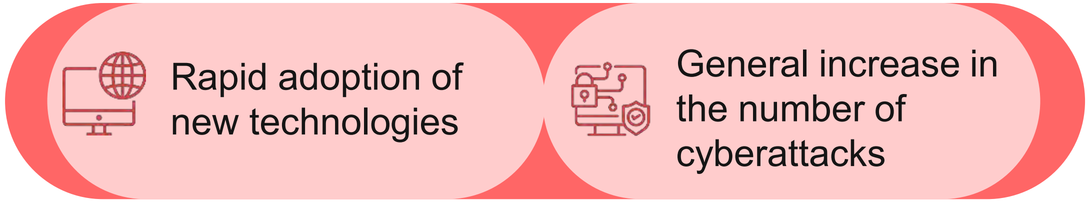
The global turnover in cybersecurity will grow at an **annual rate of 8%** during the next five years and reach **$272 B**.

Global cybersecurity turnover

(2024-2029, millions of dollars)



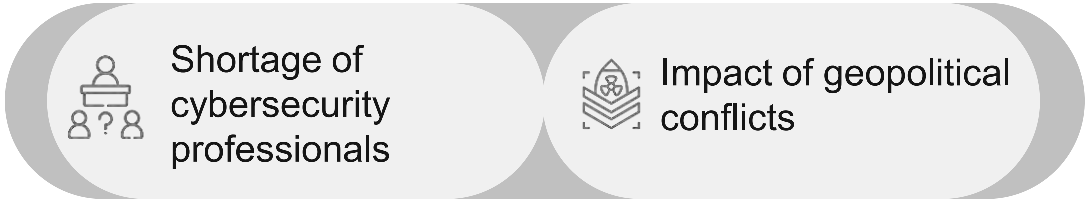
Key factors driving the growth of the cybersecurity market



Rapid adoption of new technologies

General increase in the number of cyberattacks

Main challenges facing the cybersecurity market



Shortage of cybersecurity professionals

Impact of geopolitical conflicts

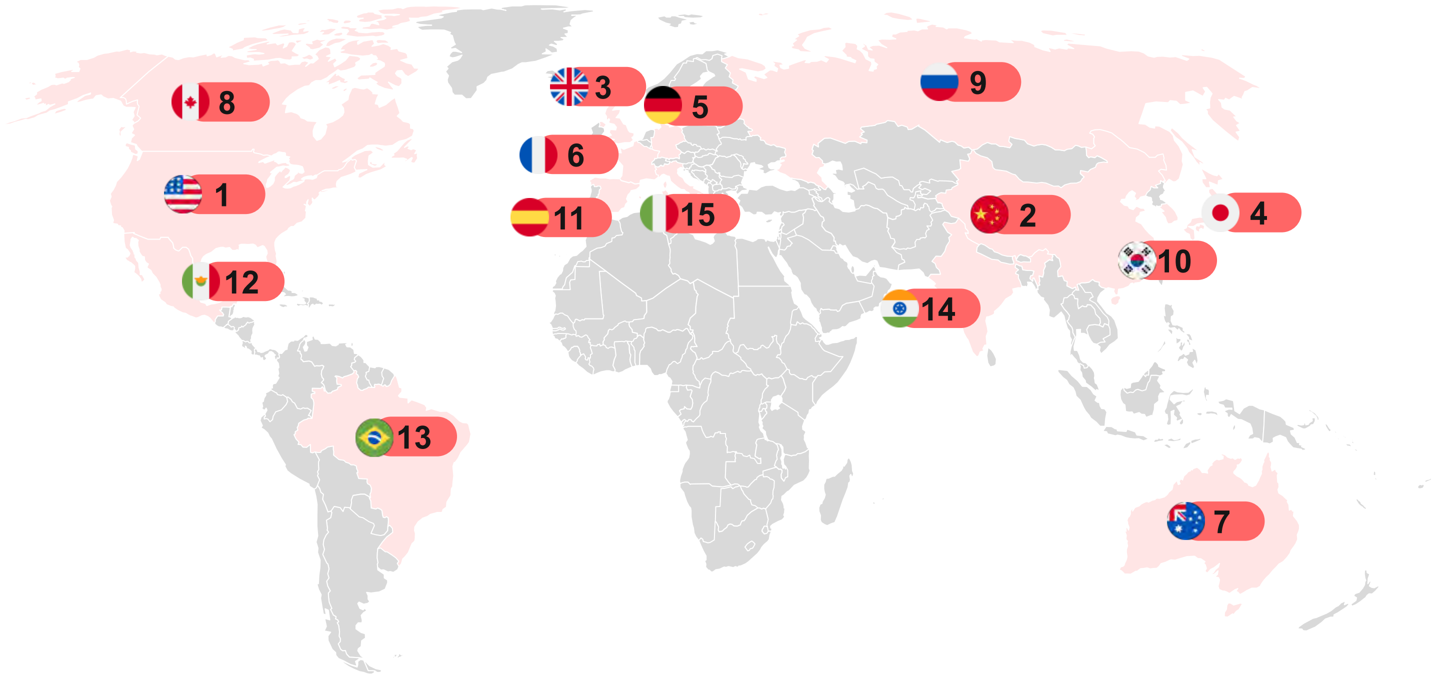
Source: Statista

Global cybersecurity market, by countries

The **United States** accounts for almost half of the global cybersecurity market

China is the second-ranked country by turnover and, together with **India**, the one that will grow the most in the coming years

Five European countries are listed in the top 15: the **United Kingdom**, **Germany**, **France**, **Spain** and **Italy**



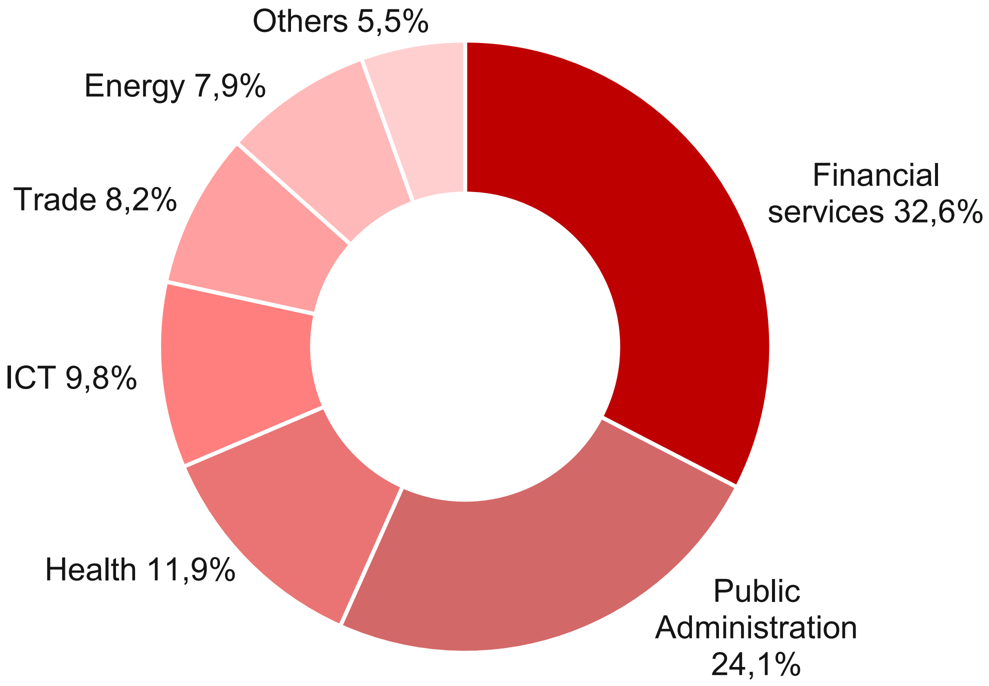
	Countries	Turnover ($M, 2024)	% annual growth 24-29
1	United States	81,370	7.4%
2	China	14,750	10.8%
3	UK	10,990	8.9%
4	Japan	9,374	7.2%
5	Germany	7,543	6.9%
6	France	5,785	6.6%
7	Australia	4,043	7.4%
8	Canada	3,834	8.2%
9	Russia	3,551	5.3%
10	South Korea	3,397	7.8%
11	Spain	3,075	6.7%
12	Mexico	3,018	7.5%
13	Brazil	2,955	8.6%
14	India	2,866	13.0%
15	Italy	2,846	6.1%

Source: Statista

Sectors that require the most cybersecurity services

Financial services, the **public administration** and **health** are the sectors with the highest demand for cybersecurity services.

Cybersecurity market share, by demand sectors (%, 2023)



Source: Statista

Generalitat de Catalunya

Leading cybersecurity companies

United States

- APPGUARD
- BROADCOM
- ● CISCO
- ● CLOUDFLARE
- ● CROWDSTRIKE
- CYBERARK
- ● DXC TECHNOLOGY
- ● FORTINET
- ● f5
- FUTUREX
- ● IBM
- imperva
- KnowBe4
- ManageEngine
- ● Microsoft
- ● okta
- OneTrust PRIVACY, SECURITY & GOVERNANCE
- ● netskope
- NordLayer
- ● paloalto NETWORKS
- ● proofpoint.
- RAPID7
- Raytheon Technologies
- RSA
- SecurityHQ
- ● Symantec A Division of Broadcom
- tenable
- Trellix
- VIPRE SECURITY GROUP
- UnderDefense CYBERSECURITY
- zscaler

United Kingdom

- DARKTRACE
- intruder
- SAPPHIRE
- softcat
- SOPHOS

Germany

- Avira
- secunet
- ● T

Israel

- CHECK POINT
- perimeter 81

France

- ● THALES
- ● Capgemini
- ● EXCLUSIVE NETWORKS

Sweden

- yubico

Czech Republic

- Avast

Spain

- ● cipher a PROSEGUR company

Canada

- Genetec

Ireland

- ● accenture

Japan

- ● TREND MICRO

India

- INDUSFACE

Poland

- ANDERSEN

● Presence in Catalonia

Source: the authors, based on eSecurity Planet, fDi Markets, Indexsy, Software Testing Help and Statista

3. Prospective applications by demand sector

Demand sectors (I)

European Directive NIS 2 determines **11 highly critical core sectors** and **7 additional important sectors** that will constitute new demand sectors for cybersecurity products and services. By 17 April 2025, the member States must have drawn up a list of the impacted entities and they must review it at least every two years.

11 highly critical core sectors, according to European Directive NIS 2

Energy

Entities dedicated to the production and transmission of electricity, heating and cooling operators, and stakeholders in the extraction and distribution of oil, gas and hydrogen.

Transport

Authorities, operators and infrastructure managers linked to air, rail, maritime and road transport.

Banking

Credit institutions.

Financial market infrastructures

Operators of business and exchange points and central counterparties (CCPs).

Health

Health service providers, EU reference laboratories, entities that carry out research and development activities for medicinal products, entities that manufacture basic pharmaceutical products and pharmaceutical preparations, and entities that manufacture medical devices considered critical during a public health emergency.

Drinking water

Suppliers and distributors of water intended for human consumption.

Wastewater

Companies that collect, remove or treat urban wastewater, household wastewater or industrial wastewater, excluding companies whose collection, disposal or treatment of wastewater is a non-essential part of their general activity.

Digital infrastructure

Internet exchange point providers/DNS service providers (excluding root domain name server operators)/TLD name registries/Cloud computing service providers/Data center service providers/ Providers of content distribution networks/Trusted service providers/Providers of publicly available electronic communications networks and services.

ICT service management (B2B)

Managed service providers (MSP) and managed security service providers (MSSP).

Public Administration

Public administration entities of central governments and at a regional level.

Space

Operators of terrestrial infrastructures, properties managed and operated by Member States or by private parties, which support the provision of space-based services (excluding providers of public electronic communications networks).

Demand sectors (II)

SMEs are becoming active consumers of cybersecurity to address the emerging cyberthreats.

In 2024, **74%** of ransomware attacks have targeted companies with 1,000 or fewer employees. This constitutes an increase of **7** percentage points with respect to 2023.

Phishing as an entry vector is used in **45%** of attacks aimed at SMEs.

20% of all companies cannot recover data after a cyberattack.

Losses from cyberattacks amount to an average of **€50,000** for smaller companies.

During the period from 1 January to 30 April 2024, a total of **2,402** cases of malware and unwanted software hidden in software products for SMEs were detected, **8%** more than in 2023.

What are the first steps to be followed?

1. Request the Digital Kit: This is a program designed for SMEs and freelancers to accompany organizations in their digital transformation process that includes various digital solutions, such as **secure communications** and **cybersecurity**.
2. Secure access: Define a policy with **complex passwords,** implement **2FA** and define the identity management for the organization.
3. Good digital practices in the digital environment: **Raise awareness and train** employees with regard to the need to follow **advice and preventive measures**, following the ten tips for good digital practices in the work environment defined by the Cybersecurity Agency of Catalonia.
4. Use of a VPN: Create a **virtual private network** to allow the user to connect securely to the internal network and the Internet.
5. Corporate digital responsibility: Maintain a **sustainable digital** environment to uphold a strategy which is beneficial for the environment, cybersecurity and the company's reputation.

Sources: Coveware, Hodeitek, Hiscox, Futurum, Securelist

Generalitat de Catalunya

Convergence of technologies with cybersecurity

Cybersecurity is evolving as it faces new threats, and it is doing so by hybridizing with complementary technologies.

- Generative artificial intelligence
- Zero day detection and protection with AI
- IoT with AI
- Post-quantum encryption

- Hybrid environments
- Observability
- Biometric technology
- 6G connectivity

4. Trends in cybersecurity and their impact on the SDGs

Main trends in cybersecurity in 2024

Deepfakes threaten the integrity and stability of electoral processes. The union between impersonating celebrities through deepfakes and their ease of distribution on social media has become a real threat to democracy.

Rise in the use of biometric data: greater security or a concern? The use of biometric data can reinforce security through the surveillance of people, but it raises concerns about privacy and the risks of digital impersonation.

The rise in the value of cryptocurrencies attracts cybercriminal activity. The increase in the value of cryptocurrencies has triggered cyberattacks to steal cryptoassets, making it essential to reinforce the security of users and platforms.

Cyberattacks in the financial sector, on the rise. The financial sector brings together valuable assets, in such a way that it attracts cyberattacks aimed at banking institutions, involving sophisticated attacks, and users, through advanced banking Trojans.

Ransomware as a service (RaaS): resistance to payments and tensions among cybercriminals. Resistance to ransomware payments is causing tensions in the RaaS model, driving the number of attacks and the migration of cybercriminals towards other groups.

Cyberattacks on supply chains cause massive data leaks on a global scale. 165 companies affected by the historic data leak at Snowflake, caused by the use of stolen credentials and the absence of two-factor authentication (2FA).

Increase in targeted fraud fueled by massive data leaks. Fraud intensifies during the holiday period through scams that offer attractive but false offers for tickets to events and summer accommodation.

Alliances between cybercriminal groups intensify cyberattacks with direct effects on Catalonia. Alliances between cybercriminal groups such as the Holy League have intensified DDoS attacks on European countries and NATO allies.

Intensification of cyberwarfare in the conflict in the Middle East. Traditional cyberattacks (DDoS, wipers and disinformation) have given way to destructive attacks with an impact on the physical world, such as the explosion of pagers targeting Hezbollah.

Cybercriminals target mobile devices for their scams. Cyberfraud uses mobile phones as its main entry vector, combining attacks via email, SMS, social media and voice calls to deceive its victims.

Data theft remains a headache in the healthcare sector. The theft of personal and medical data from the healthcare sector, often through ransomware attacks, involves extortion with the threat of publishing them and leaking sensitive data.

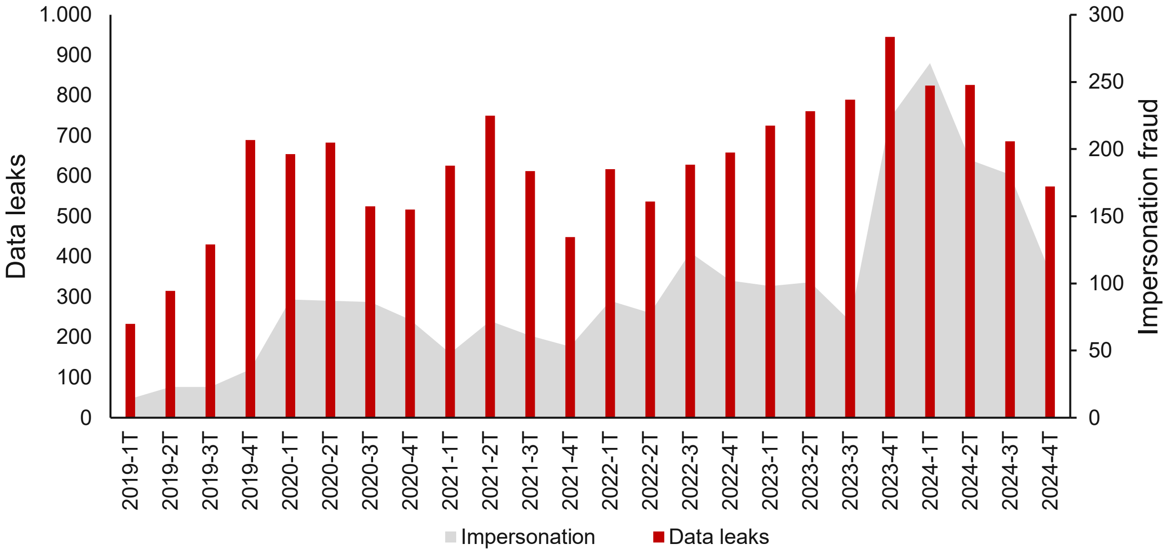
2024, a record year for ransomware. 2024 has set a record for the number of ransomware incidents, with attacks focused on critical sectors, demonstrating that cybercriminals are capable of industrializing them.

Source: Cybersecurity Agency of Catalonia

Main cybersecurity trends in 2024: data leaks lead to a rise in cyberfraud, which becomes more sophisticated

Personal data leaks are fueling the black market and allowing cybercriminals to craft sophisticated, targeted and credible cyberscams.

Evolution of the number of news stories about data leaks and cyberfraud through impersonation (2019-2024)



There exists a correlation between the number of news stories about data leaks and the number of impersonations. Thus, after a peak in data leaks, there is an increase in impersonation fraud.

In 2024 there has been an increase in the number of data leaks providing attackers with access to large amounts of sensitive information, including personal, financial, and business data.

The compromised data are sold on the dark web and allow fraud mechanisms through different media (multi-channel scams) or by combining the physical and digital worlds (hybrid scams) to make them more credible.

The compromised data are used to send phishing, smishing and vishing attacks with the aim of obtaining credentials. These credentials are used to log into personal accounts to perform impersonations and steal valuable assets.

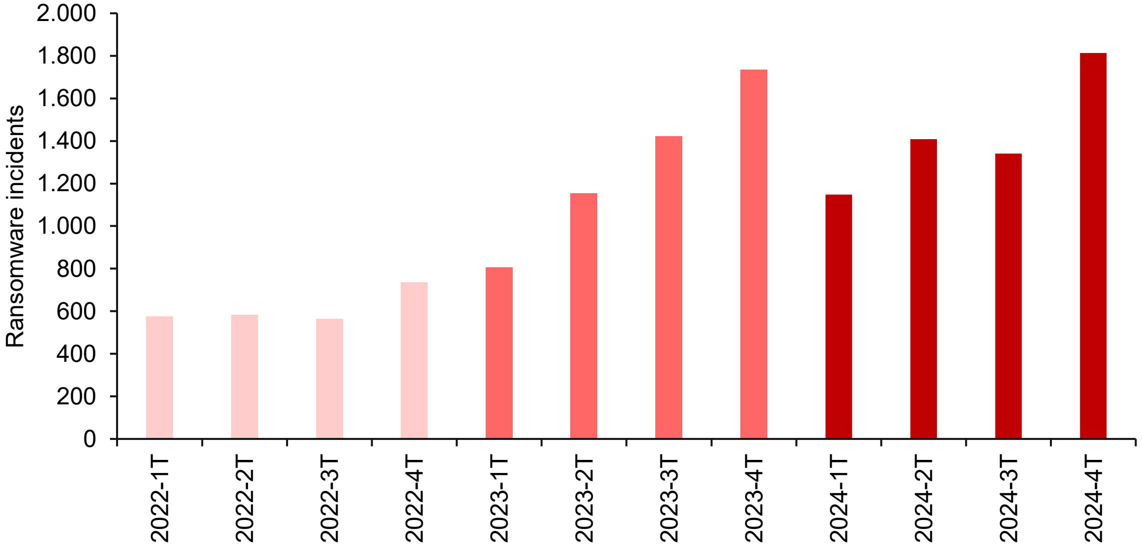
Cybercriminals use generative artificial intelligence to massively produce messages with well-written texts, in any language and suited to each potential victim to increase the likelihood of success.

Source: Cybersecurity Agency of Catalonia

Main cybersecurity trends in 2024: more ransomware incidents, more cybercriminal groups and more data theft

The fall in the number of ransomware victims that make payments has encouraged cybercriminal groups to increase their attacks and extort their victims with stolen data.

Evolution of the number of ransomware incidents (2022-2024)



During 2024, 11% more ransomware incidents than in 2023 have been detected, with 133% more than in 2022.

The percentage of ransomware victims that make payments is falling and, in response, cybercriminals are increasing their activity to preserve their income.

The fall in the percentage of payments has created internal tensions among the criminal groups, leading to the creation of new ones. This year, up to 48 new ransomware groups have been counted, more than in any other year.

The ransomware groups have also increased their profits stemming from data theft. Currently, the ransomware players not only encrypt data, they also steal them and then seek to profit from them through extortion and selling them on the dark web.

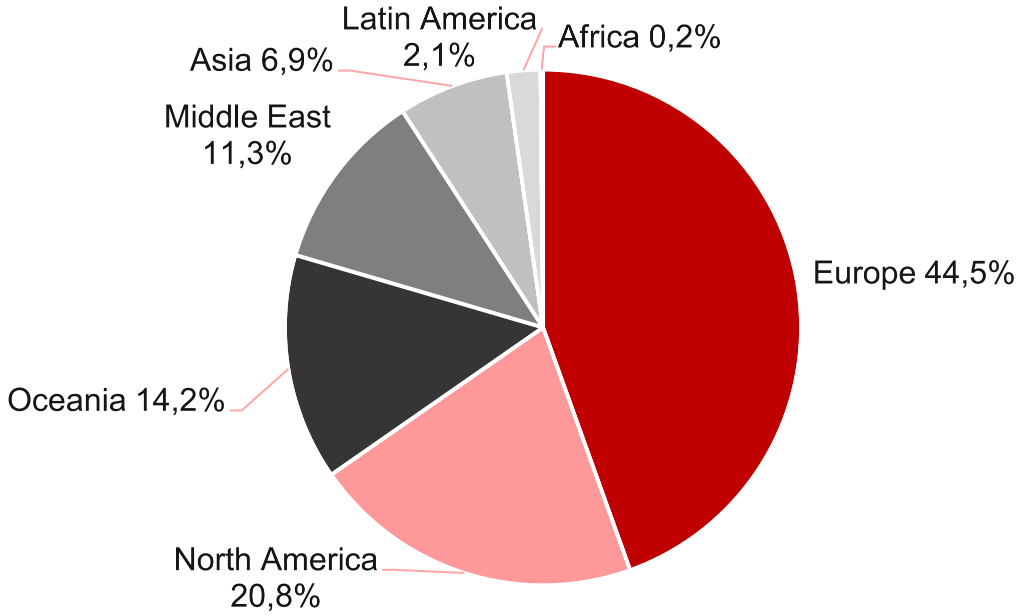
Ransomware attacks are becoming massive and affecting all kinds of organizations, even SMEs. These companies often have fewer resources to invest in cybersecurity, making them more vulnerable targets.

Sources: Cybersecurity Agency of Catalonia, RansomDB

Main cybersecurity trends in 2024: rising geopolitical tensions drive DDoS attacks against Europe

Geopolitical cyberattacks have evolved from espionage to destructive actions and disinformation, affecting not only countries in conflict, but also those that adopt ideologically aligned positions.

Distribution of DDoS attacks by regions (2024)



In 2024, Europe is the region that has been most affected by DDoS attacks, above North America, the one most affected until now.

Geopolitically motivated attacks are being used by groups and nations to destabilize adversaries, in order to demonstrate their power through propaganda or access confidential and personal information.

DDoS attacks have predominated in 2024: different organized cybercriminal groups with an ideology opposed to NATO have created an alliance (DDoSia Project) to attack the availability of websites in different countries to generate propaganda.

Within the context of geopolitical conflicts, the cyberattacks target both countries in conflict and those that are not directly involved but have adopted a public stance. Cyberwars have no borders.

In the geopolitical sphere, destructive cyberattacks with an impact on the physical world and people's lives have risen in number. One example of the above is the detonation of electronic devices in the Middle East and the hundreds of victims.

Source: Cybersecurity Agency of Catalonia

Relevant events in 2024

INTERNATIONAL		CATALONIA
McAfee presents an AI shield to combat audio deepfakes AI	Jan. 24	Veolia, the owner of Aigües de Barcelona, is the victim of a ransomware attack *Ransomware*
Scammers use a deepfake to steal 25 million dollars Fraud	Feb. 24	Iris scanning in exchange for cryptocurrencies at Catalan shopping centers Privacy
An unprecedented cyberattack on 800 French ministry websites DDoS	March 24	Alert regarding a fraudulent SMS campaign by the Tax Agency to return money Fraud
AT&T confirms a data leak involving 73 million customers Data leak	April 24	A cyberattack compromises the personal data of Catalan families and schools Data leak
The University of Siena, a victim of ransomware Ransomware	May 24	Dismantling of a cybercriminal network on the Costa Dorada Police actions
A cyberattack on Snowflake causes a historic data leak Data leak	June 24	The Republican Left party, a target for cyberattackers Data leak
A ransomware cyberattack paralyzes 40 museums during the Olympic Games Ransomware	July 24	Groups affiliated to the DDoSia project attack the websites of Catalan institutions DDoS
The FBI dismantles a Russian bot farm that spreads disinformation on a global scale Police actions	August 24	The Catalan healthcare service, paralyzed by the CrowdStrike incident Availability
A ransomware attack forces the temporary closure of a school in the United Kingdom Ransomware	Sept. 24	The Waste Agency of Catalonia suffers a cyberattack Ransomware
The developer of Pokémon, the victim of a cyberattack that leaks more than 1TB of data Data leak	Oct. 24	An impersonation scam costs the victim a total of €23,000 Fraud
Memorial Hospital and Manor, the victim of a ransomware attack Ransomware	Nov. 24	Investigation into data theft in the *La Meva Salut* application Credential theft
New tactics for deploying ransomware attacks Ransomware	Dec. 24	A criminal organization that impersonated banks is dismantled in Osona Police actions

Source: various sources

Cyberattack figures with an impact on Catalonia in 2024

4%

Cyberincidents are on the rise in Catalonia

The number of reported cybersecurity incidents in Catalonia has increased by 4% compared to the previous year.

3%

Less ransomware in the public sector

According to the APDCAT, the register of ransomware attack notifications has recorded a fall from 19% last year to 3% in the current one.

35%

Citizens' awareness of their rights

This year the APDCAT has received 35% more reports and claims regarding breaches of the data protection regulation.

60%

Most data leaks are due to human error

According to the APDCAT, 60% of data leaks at Catalan public institutions have been caused by human error.

1st

Catalonia, the leader in reports of cyberscams

Catalonia was the autonomous community with the most reports of computer scams, with a total of 71,772.

95%

Prevalence of computer scams

The computer scams reported in Catalonia account for 95% of all recorded cybercrime.

67%

Fraudulent bank charges are the most common cyberscams

News stories concerning financial fraud affecting citizens have risen by 55% compared to the previous year.

24%

Infected IPs in Catalonia

24% of the infected IPs in Catalonia are derived from the RootSTV malware designed for Smart TVs with old Android versions.

Sources: APDCAT, Bitsight, Catalan Police Force, Cybersecurity Agency of Catalonia

Main milestones for 2025

Cyberscams

- Personal data leaks have occurred at an alarming rate, a situation that augurs a 2025 full of cyberscams, which, thanks to the use of these data, will become increasingly sophisticated. As a result of artificial intelligence (AI), the scams may be personalized and massive.

Artificial intelligence

- AI will also be key to cybersecurity in the fight against complex cyberattacks, as it can provide advanced detection and automatic response tools. This technology will be able to improve network security and the early detection of suspicious behavior.

Supply chains

- The increased connectivity and complexity of supply chains will facilitate cyber risks. Manufacturers and organizations will continue to embrace the adoption of zero-trust cybersecurity models.

Geopolitics

- The growing number of geopolitical conflicts will fuel a new wave of destructive cyberattacks, including DDoS and wipers and other variants demonstrating their ability to cause real damage to the physical world.

Ransomware

- Ransomware is probably the most significant cyberthreat for organizations and it will continue to evolve in order to maintain its income. Extortion through data theft, during which the information is encrypted and a threat to disclose it is made, will become an effective practice.

Regulations

- The cybersecurity regulation will require new cybersecurity requests, in keeping with the emerging cyberthreats. For all kinds of organizations, 2025 will be a key year for adapting to significant new cybersecurity regulations.

Source: Cybersecurity Agency of Catalonia

5. Quantum and cybersecurity

Quantum technologies

Quantum technologies are a series of emerging technologies that take advantage of the principles of quantum mechanics, a branch of physics that describes the behavior of matter at atomic and subatomic levels.

Quantum computing is an emerging technology that takes advantage of the laws of quantum mechanics to solve problems that are too complex for traditional computers. Complex problems are ones with many variables that interact in complicated ways. These machines are very different from the classic computers that have existed for more than half a century.

Quantum communication is a field of applied quantum physics closely related to quantum information processing. It involves encoding information in quantum states of light for the transmission of information and enabling disruptive cryptography applications.

Quantum communication encompasses a wide range of technologies and applications ranging from state-of-the-art laboratory experiments to commercial reality. It has some of the most mature quantum technologies in quantum key distribution (QKD) and quantum random number generators (QRNG).

Within quantum technology, a **quantum sensor** uses the properties of quantum mechanics, such as quantum entanglement, quantum interference, and quantum state narrowing, which have optimized accuracy and overcome the current limitations of sensor technology. This technology detects changes in movement with great precision, including magnetic and electric fields, greatly improving the ability to measure and understand the environment.

Source: the authors, based on IBM, MIT Technology Review, Quside and PwC: Quantum Technology Monitor

Impact of quantum technologies on cybersecurity

Quantum technologies may pose a threat to current data encryption, but they can also improve cybersecurity.

Quantum computers pose a significant threat to the current encryption standards, including RSA and ECC, which protect numerous communications and a large amount of data.

Algorithms such as that of Shor allow quantum computers to break through these encryption methods, potentially compromising sensitive data around the world.

Quantum technologies can improve cybersecurity through innovations such as quantum key distribution (QKD) and quantum random number generation (QRNG), providing ultra-secure communication and stronger cryptographic methods. Meanwhile, post-quantum algorithms protect data storage.

Solutions for the quantum risk

Post-quantum cryptography

Development and implementation of quantum security algorithms that are secure in the event of computer-supported quantum attacks.

Regarded as the leading solution for quantum threats to encryption, due to its familiarity as an extension of current systems.

Secure in the event of known quantum attacks.

Deployable within the existing infrastructure.

Known PQC schemes have drawbacks in terms of their performance, including long keys and extended processing times.
Cryptanalysis developments may affect their security in the future.

Quantum key distribution (QKD)

QKD enables two parties to create a shared secret key to encrypt and decrypt messages. Any attempt to interfere with the quantum communication will be detected.

Increased protection against “harvest now, decrypt later” attacks, given that the key exchange protocol is not vulnerable to quantum attacks.

It can be combined with other schemes for greater security.

No algorithms can be developed to access the exchanged keys.

Major investment in specialized hardware.
Potential distance-related imitations, pending the development of a satellite quantum/QKD repeater.
Requires a separate authentication channel, adding complexity.

Quantum Random Number Generators (QRNGs)

QRNGs generate truly random numbers through nondeterministic processes, offering a higher degree of security in data encryption.

While classical RNGs (random number generators) stem from an entropy source (such as thermal noise), QRNGs are inherently random.

The possibility of testing the randomness (certifiable randomness) for certain implementations.

Some applications require repeatability, which is not possible with QRNGs.
It is difficult to quantify the improvement in security.

Source: the authors, based on KPMG, Deloitte, CEPS (Center for European Policy Studies), Telefónica and World Economic Forum

Raise awareness of the quantum threat and understand the risk

01.

Cryptography

Review cryptographic systems to create a dynamic infrastructure adaptable to the changing business and security needs.

02.

Cryptoagility

Create tools to efficiently update cryptographic algorithms, parameters, and technologies whenever necessary.

03.

Cybersecurity ecosystem

Collaboration with the administration, associations and industry to learn more about advances in quantum computing, cryptography and risks.

04.

Cybersecurity hygiene

Protect sensitive data from all kinds of threats, including the future risks caused by quantum computing. While the threat may seem distant, organizations must balance their investments in quantum risk mitigation with other cybersecurity priorities.

Source: the authors, based on KPMG, Deloitte, CEPS (Center for European Policy Studies), Telefónica and World Economic Forum

6. Initiatives in cybersecurity

Cybersecurity in the European Union

The European Union deploys its cybersecurity capabilities with several approaches:

European Cybersecurity Strategy

Presented in 2020, the EU’s Cybersecurity Strategy reinforces the collective response to cyberattacks, protects essential services, promotes technological autonomy and drives international cooperation to ensure security in cyberspace.

Legislation and certification

- Directive on the security of networks and information systems (NIS Directive)
- Cyber Resilience Regulation
- Cybersecurity Act
- Cybersolidarity Regulation

Investment

- Next Generation
- R+D+I: Horizon Europe
- Digital Europe Program
- InvestEU

Regulatory guidance

- Master plan for a coordinated response to major cyberattacks
- Joint Cyber Unit
- Secure deployment of 5G in the EU
- Guarantee electoral processes

Skills and sensitization

Faced with a shortage of cybersecurity experts, the European Commission is taking measures to stimulate the development of cybersecurity capabilities, including the Cybersecurity Skills Academy launched in 2023.

Cyber-community

- ENISA
- ISAC (Information Sharing and Analysis Center)
- JRC (Joint Research Center)
- CSIRT/CERT (Computer Security Incident Response Teams)
- ECSO (European Cybersecurity Organization)
- Women4Cyber

Cyberpolitics

- Cyberdiplomacy
- Cyberdefense
- Development of skills in third countries
- Cyberdialogs with partners such as the USA, Ukraine and Japan.

Source: European Commission

New European cybersecurity regulation (I)

Cyber Resilience Regulation

The Cyber Resilience Regulation is a European Union standard that seeks to protect consumers and companies that purchase or use products with a digital component.
The law guarantees the following:

- Harmonized standards for the marketing of computer products and programs with a digital component.
- A framework of cybersecurity requirements that govern the planning, design, development and maintenance of products, with obligations that must be met in all of the phases of the value chain.
- Obligation to ensure the entire life cycle of the products.

This standard affects the manufacturers and retailers of all products directly or indirectly connected to another device or network, with certain exceptions.

The regulation entered into force on 10 December 2024 and it will become generally applicable on 11 December 2027.

Digital Operational Resilience Act (DORA)

This regulation is a European Union standard to regulate the way in which financial institutions manage the digital risk in finance.
The standard impacts the following issues:

- In-house and third-party ICT risk management.
- ICT-related incidents and notifications of incidents.
- Digital operational resilience tests, including a range of assessments, trials, methodologies, practices and tools.
- Exchanges of information between financial institutions.
- Continuous monitoring of the functioning of systems and tools.

This standard affects, among others, the following companies:

- Credit institutions.
- Payment and electronic money institutions.
- Investment service institutions.
- Cryptoasset service providers.
- Other financial institutions: fund managers, insurers, etc.

The regulation has been fully applicable since 17 January 2025.

New European cybersecurity regulation (II)

National Security Scheme (ENS)

The ENS is a Spanish regulation that seeks to:

- Create the security conditions required for the use of electronic media.
- Promote continuous security management.
- Promote prevention, detection and correction.
- Promote homogeneous treatment of security.
- Serve as a model for good practices.

This standard affects the entire public sector (in accordance with article 2 of Law 40/2025), as well as systems that handle classified information (without detriment to Law 9/1968 on Official Secrets). It also applies to the information systems of private sector entities that offer services and solutions to public sector entities.

The National Security Scheme is regulated by Royal Decree 311/2022, of 3 May, and the affected systems have to adapt to it within the period of 24 months after the regulation came into force on 3 May 2024.

Network and Information Systems Directive 2 (NIS2)

The NIS 2 Directive is a European Union standard that seeks to provide a higher common degree of cybersecurity, taking into account the importance of network and information systems for the economy and society.

The Directive encompasses procedures that include:

- Risk management.
- Incident management.
- Supply chain security.

This standard affects medium-sized and large entities in sectors critical to the economy and society, including providers of public electronic communications services, digital services, wastewater and waste management, the manufacture of critical products, postal and courier services, the public administrations, the public supply entities of autonomous communities and local public administration entities.

By 17 April 2025, the member States must have drawn up a list of the impacted entities and they must review it at least every two years.

7. Cybersecurity in Catalonia

Business mapping of cybersecurity in Catalonia (I)

557 companies

+7.9%[1]

1.473 billion euros

+18.4%[1]

10,672 jobs

+12.8%[1]

82.6% are SMEs.

57.1% bill more than 1 million euros and **22.6%** bill over 10 million euros.

26.0% are less than 10 years old.

10.6% are startups.

26.4% are exporters.

16.9% are foreign subsidiaries.

By **segments**, the companies:

Protect	**90.3%**
Identify	**62.5%**
Detect	**41.8%**
Respond	**35.5%**
Recover	**23.0%**

238 companies (42.7%) also develop solutions linked to **artificial intelligence**

[1] the growths are in comparison with the mapping data for the previous year.

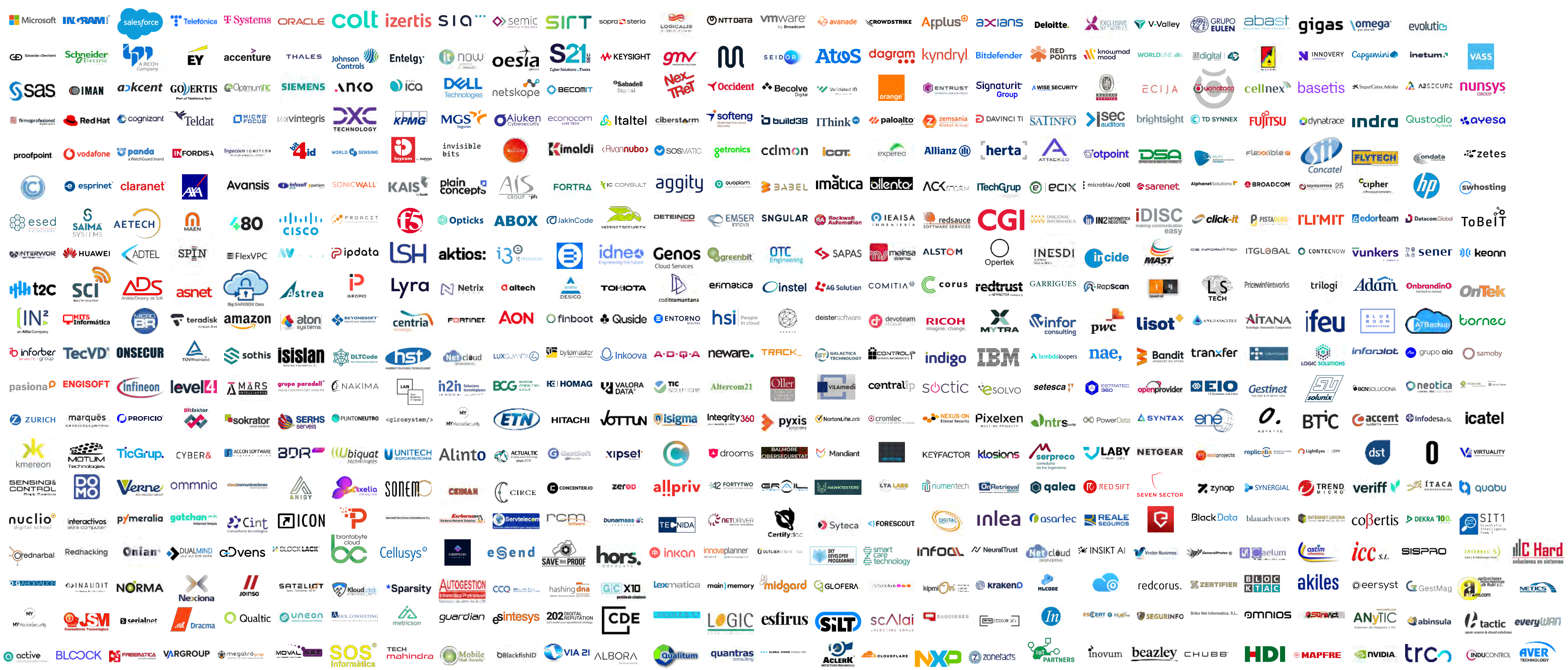
Note: the company data refer to 2024 and the billing data and the number of employees refer to 2023 (or the latest available year).

Source: ACCIÓ

Business mapping of cybersecurity in Catalonia (II)

Full mapping

557 companies



Business mapping of cybersecurity in Catalonia: identify segment

Identify

348 companies

Microsoft · INGRAM · Telefónica · T Systems · ORACLE · SIA · semic · sopra steria · LOGICALIS · NTT DATA · vmware by Broadcom · avanade · CROWDSTRIKE · Applus+ · axians · Deloitte. · V-Valley · GRUPO EULEN · abast

omega · evolutio · Giesecke+Devrient · Schneider Electric · EY · accenture · THALES · Johnson Controls · Entelgy · oesía · S21sec · KEYSIGHT · gmv · SEIDOR · Atos · dagrama · kyndryl · Bitdefender · RED POINTS

knowmad mood · digital · INNOVERY · Capgemini · inetum. · IMAN · ackcent · GOVERTIS Part of Telefónica Tech · OptimumTIC · SIEMENS · ANKO · BECOMING · Sabadell · NexTReT · Occident · Becolve Digital · ENTRUST · WISE SECURITY · BUREAU VERITAS

ECIJA · SegurCaixa Adeslas · nunsys group · Red Hat · cognizant · Teldat · vintegris · DXC TECHNOLOGY · KPMG · Aiuken Cybersecurity · Italtel · softeng · build38 · IThink · paloalto · zemsania Global Group · isec auditors · brightsight · FUJITSU

dynatrace · indra · ayesa · panda a WatchGuard brand · INFORDISA · Avannubo · SOSMATIC · getronics · cdmon · icot · expereo · otpoint · DSA · S2 GRUPO · Concatel · zetes · claranet · esprinet

AXA · Avansis · infoself group · parlem · plain concepts · FORTRA · aggity · BABEL · imàtica · ACKSTORM · ecix · microblau/colt · Alphanet Solutions · BROADCOM · sayoscarrera 25 · hp · swhosting · esed · AETECH · 480

CISCO · PROACIT · Opticks · ABOX · JakinCode · DETEINCO · Rockwell Automation · IEAISA INGENIERIA · redsauce SOFTWARE SERVICES · CGI · click-it · I'LIMIT · edorteam · Datacom Global · ToBeIT · HUAWEI · SPIN · AV cloud · aktios:

i3e it resources · idneo Engineering the future · Genos Cloud Services · greenbit · ALSTOM · Opertek · incide · ITGLOBAL · CONTECNOW · vunkers · sener · SCI · ADS · asnet · Big SAFEBOX Data · INFOPID · Netrix · altech

DESICO · coditramuntana · efimatica · instel · AG Solution · corus · redtrust a KEYFACTOR company · GARRIGUES · LS TECH · OnbrandinG · OnTek · IN2 an Altia Company · MTS Informática · teradisk Grupo Aire · amazon · BEYONDSOFT · centria · Quside · ENTORNO DIGITAL

ARONTE · deistersoftware · MYTRA · infor consulting · pwc · lisot · AITANA · borneo · inforber group · TecVD · ONSECUR · TÜVRheinland · sothis · isislan · DLTCode · hst · Netcloud · Inkoova · A·D·Q·A

TRACK_ · GALACTICA TECHNOLOGY · indigo · IBM · nae, · Bandit · LOGIC SOLUTIONS · inforplot · samoby · pasiona · ENGISOFT · Infineon · MARS · grupo paradell · i2n · BCG BOSTON CONSULTING GROUP · TIC SOLUTIONS · Altercom21

centralip · sctic · esolvo · setesca · ESTRATEC 360 · openprovider · EIO · Gestinet · BCNSOLUCIONA · infoserveis · Wolters Kluwer · ZURICH · PROFICIO · sokrator · VOTTUN · pyxis · NEXUS-ON Ethical Security · Pixelxen · ntrs · PowerData

SYNTAX · O. ADVANTIC · BTIC · infodesa SL · kmereon · MOTUM · TicGrup · CYBER& · ACCON SOFTWARE · BDR GROUP · UNITECH IBEROAMERICANA · GestSoft · xipset · BALMORE CIBERSEGURETAT · Mandiant · INFOCOM · LABY forever data · essiprojects

LightEyes · La Salle · dst · 0 · VIRTUALITY · DOMO · Verne TECHNOLOGY GROUP · ANIGY · axelia · CONCENTER.IO · allpriv · GRAIL TECH · HAWKTESTERS · numentech · OnRetrieval · SEVEN SECTOR · zynap · SYNERGIAL · TREND MICRO · veriff

ÍTACA · interactivos · pymeralia · gatchan · Cint Consultoria tecnològica · ICON · P · Servitelecom · Dunamass · NETDRIVER · DIGITAL · inlea · asartec · BlackData · blauadvisors · INTERNET GIRONA · DEKRA 100 · redarbal

Redhacking · Devens · BLOCKLACK · Cellusys · eSend · SAVE THE PROOF · hors. advocats · innovaplanner · OUTLIER CONSULTING · SKY DEVELOPER PROGRAMMER · NeuralTrust · GeneralProtec · astim · DGA ABOGADOS · INAUDIT · NORMA · JOINSO · Kloud click

AUTOGESTION Informática Profesional · CCQ · hashing dna · GC X10 · lexmatica · midgard · GLOFERA · iAmOnChain · kipmiOn · MLCODE · ZERTIFIER · peersyst · aplicaciones informáticas de Rubí s.l. · JSM Consultoria Tecnològica · Qualtic · uneon · ARIOL CONSULTING · metricson · 202 DIGITAL REPUTATION

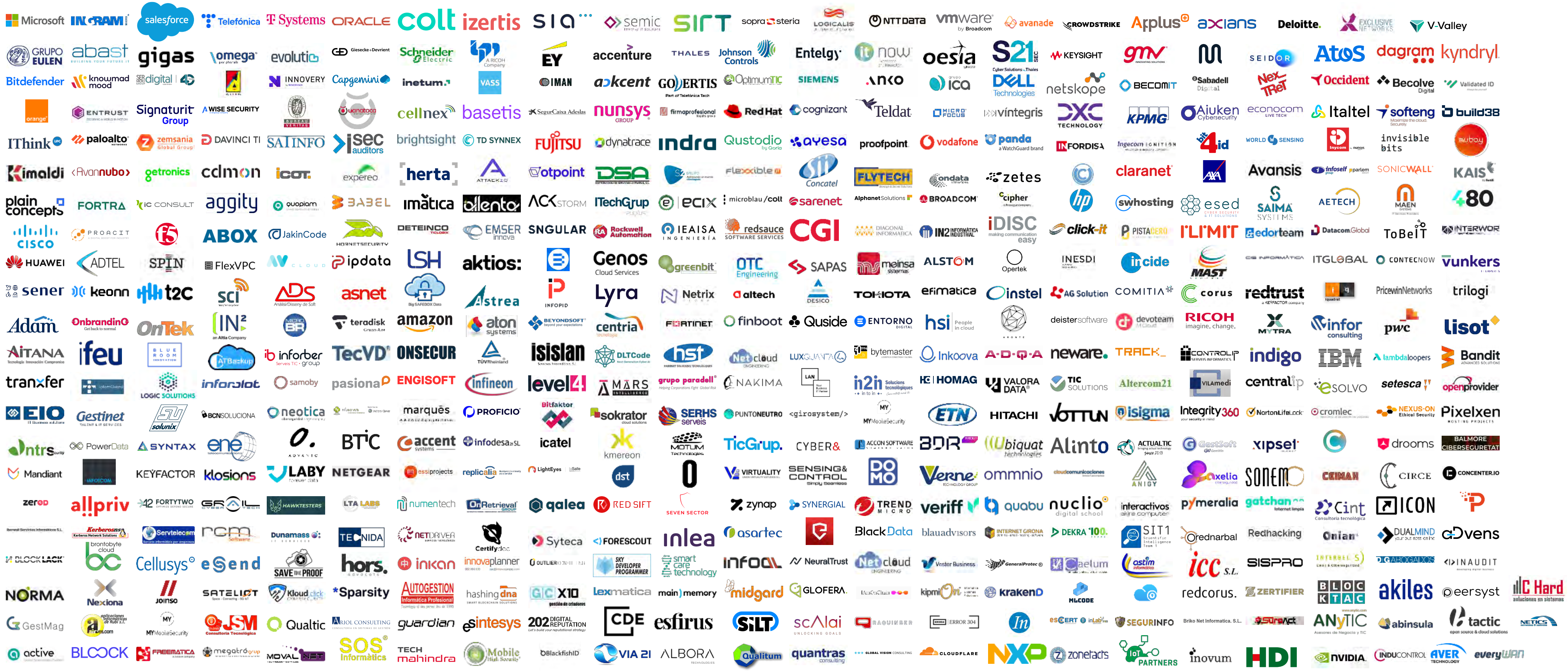
CDE · LOGIC · SILT · scAlai UNLOCKING GOALS · RAQUIMBER · ERROR 304 · In · esCERT · inLab · SEGURINFO · Briko Net Informatica, S.L. · omnios · SureAct · ANyTIC · abinsula · FREEMATICA · MOVAL NET · SOS Informàtics · TECH mahindra

Qualitum · quantras consulting · GLOBAL VISION CONSULTING · CLOUDFLARE · HDI · NVIDIA · INDUCONTROL · AVER TECHNOLOGY · everyWAN · NETICS · IC Hard

Business mapping of cybersecurity in Catalonia: protect segment

Protect

503 companies



Generalitat de Catalunya

Business mapping of cybersecurity in Catalonia: detect segment

Detect

233 companies

- Microsoft
- Telefónica
- T Systems
- ORACLE
- SIA
- semic
- SIRT
- NTT DATA
- vmware by Broadcom
- CROWDSTRIKE
- axians
- Deloitte.
- abast
- evolutio
- Giesecke+Devrient
- EY
- accenture
- THALES
- Johnson Controls
- Entelgy
- oesia
- S21sec Cyber Solutions by Thales
- KEYSIGHT
- gmv
- SEIDOR
- Atos
- dagram
- kyndryl
- Bitdefender
- RED POINTS
- knowmad mood
- WORLDLINE
- SBdigital | 4D
- AITEN
- INNOVERY
- Capgemini
- VASS
- sas
- IMAN
- a>kcent
- SIEMENS
- grupo ica
- netskope
- BECOMIT
- Sabadell Digital
- NexTReT
- BUREAU VERITAS
- basetis
- A2SECURE
- nunsys GROUP
- Teldat
- MICRO FOCUS
- KPMG
- Aiuken Cybersecurity
- Italtel
- ciberstorm
- softeng
- build38
- IThink
- paloalto networks
- zemsania Global Group
- DAVINCI TI
- isec auditors
- TD SYNNEX
- dynatrace
- indra
- ayesa
- panda a WatchGuard brand
- INFORDISA
- invisible bits
- Avannubo
- SOSMATIC
- getronics
- ATTACKIQ
- otpoint
- DSA
- S2 GRUPO
- esprinet
- claranet
- AXA
- infoself parlem
- plain concepts
- AIS GROUP pfs
- FORTRA
- iC CONSULT
- aggity
- BABEL
- ACKSTORM
- sarenet
- BROADCOM
- cipher a Prosegur company
- hp
- esed cyber security & IT solutions
- 480
- cisco
- f5
- Opticks
- ABOX
- JakinCode
- DETEINCO
- Rockwell Automation
- IEAISA INGENIERÍA
- CGI
- iDISC making communication easy
- click-it
- PISTACERO
- I'LIMIT
- ToBeIT
- HUAWEI
- ADTEL
- ipdata
- LSH
- greenbit
- ALSTOM
- Opertek
- incide
- vunkers
- sci
- ADS Anàlisi/Disseny de Soft
- Netrix
- altech
- DESICO
- instel
- corus
- RepScan
- LS TECH
- trilogi
- OnbrandinG Get back to normal
- teradisk Grupo Aire
- amazon
- aton systems
- BEYONDSOFT beyond your expectations
- centria
- Quside
- hsi People in cloud
- ARONTE
- FORTINET
- MYTRA
- pwc
- lisot
- APOLO ANALYTICS
- DLTCode
- hst
- A·D·Q·A
- indigo
- IBM
- nae,
- tranxfer
- inforalot
- grupo aia
- pasiona
- ENGISOFT
- infineon
- MARS INTELLIGENCE
- LAN Your Business IT Partner
- i2n Solucions tecnològiques
- TIC SOLUTIONS
- Altercom21
- esolvo
- setesca
- Gestinet TALENT & IT SERVICES
- BCNSOLUCIONA
- PROFICIO
- sokrator cloud solutions
- Integrity360 your security in mind
- cromlec
- PowerData
- BTIC
- icatel
- kmereon
- ACCON SOFTWARE
- 3DR GROUP
- UNITECH IBEROAMERICANA
- Alinto
- Mandiant
- LABY forever data
- LightEyes
- LaSalle
- Verne Technology Group
- ANIGY
- axelia
- SONEM
- CONCENTER.IO
- allpriv
- 42 FORTYTWO
- GRAIL
- HAWKTESTERS
- numentech
- qalea
- RED SIFT
- SEVEN SECTOR
- zynap
- SYNERGIAL
- TREND MICRO
- ITACA advanced analytics
- interactivos
- pymeralia
- ICON
- Kerberos Kerberos Network Solutions
- TECNIDA
- asartec
- Orednarbal
- Dvens
- Cellusys
- inkan
- SKY DEVELOPER PROGRAMMER
- NeuralTrust
- INSIKT AI
- GeneralProtec
- icc S.L.
- INTERBEL S)
- AUTOGESTION Informàtica Professional
- midgard
- MLCODE
- redcorus.
- ZERTIFIER
- JSM Consultoria Tecnològica
- sintesys
- 202 DIGITAL REPUTATION
- scAlai UNLOCKING GOALS
- RAQUINBER
- esCERT
- inLab
- VARGROUP
- BlackfishID
- VIA 21
- ALBORA
- GLOBAL VISION CONSULTING
- ACLERK DETECTIVES PRIVADOS S.L.
- CLOUDFLARE
- HDI
- NVIDIA
- INDUCONTROL
- AVER TECHNOLOGY
- everyWAN
- NETICS
- IC Hard soluciones en sistemas

Business mapping of cybersecurity in Catalonia: respond segment

Respond

198 companies

Microsoft · INGRAM · Telefónica · T Systems · ORACLE · colt · izertis · SIRT · NTT DATA · vmware by Broadcom · CROWDSTRIKE · axians · Deloitte. · GRUPO EULEN · Giesecke+Devrient

A RICOH Company · EY · accenture · Johnson Controls · it now · oesía grupo · S21 SEC Cyber Solutions by Thales · SEIDOR · Atos · kyndryl · Bitdefender · RED POINTS · WORLDLINE · SBS digital · INNOVERY

sas · IMAN · adkcent · GOVERTIS Part of Telefónica Tech · ANKO · DELL Technologies · BECOMIT · Sabadell Digital · NexTReT · Occident · orange · A WISE SECURITY · BUREAU VERITAS · ECIJA · cellnex

basetis · SegurCaixa Adeslas · Teldat · DXC TECHNOLOGY · grupo ica · KPMG · MGS Seguros · Aiuken Cybersecurity · econocom LIVE TECH · ciberstorm · build38 · zemsania Global Group · isec auditors · indra · getronics

cdmon · icot · Allianz · DSA · S2 Grupo · ondata · claranet · AXA · plain concepts · aggity · imática · ACK STORM · ecix · sarenet

Alphanet Solutions · BROADCOM · cipher a Prosegur company · esed cyber security & IT solutions · AETECH · CISCO · f5 · Opticks · ABOX · JakinCode · DETEINCO · Rockwell Automation · IEAISA INGENIERÍA · redsauce SOFTWARE SERVICES · DIAGONAL INFORMÀTICA

click-it · PISTACERO · LIMIT · edorteam · HUAWEI · FlexVPC · ALSTOM · INESDI · incide · ADS Análisi/Disseny de Soft · asnet · INFOPID · Netrix · coditramuntana · instel

corus · RepScan · trilogi · Adam · OnbrandinG Get back to normal · MITS Informática · teradisk Grupo Aire · amazon · FORTINET · AON · Quside · pwc · lisot · torneo

ONSECUR · DLTCode · bytemaster · A·D·Q·A · TRACK_ · CONTROLIP SERVEIS INFORMATICS · IBM · tranxfer · inforpilot · samoby · pasionaP · level4 · MARS INTELLIGENCE · i2in Solucions tecnològiques · VALORA DATA

TIC SOLUTIONS · Oller · VILAmedi · centralip · soctic · esolvo · BCNSOLUCIONA · ZURICH · ntrs security · BTIC · BDR GROUP · UNITECH IBEROAMERICANA · Alinto · ACTUALTIC

BALMORE CIBERSEGURETAT · Mandiant · serpreco correduría de los ingenieros · LABY forever data · replicalia · LightEyes · LaSalle · Verne Technology Group · axelia · GRAIL CYBER TECH · numentech · SEVEN SECTOR · SYNERGIAL · Kerberosns Kerberos Network Solutions · TECNIDA

asartec · REALE SEGUROS · cobertis · DEKRA 100 years · SIT1 Scientific Intelligence Team 1 · Advens · hors. advocats · OUTLIER CONSULTING · SKY DEVELOPER PROGRAMMER · GeneralProtec · astim informática · CCQ · Lexmatica · GLOFERA.

MLCODE · aplicaciones informáticas de Rubí s.l. · serialnet · Dracma · intesys · scAlai UNLOCKING GOALS · In · esCERT · inLab · Briko Net Informatica, S.L. · active · VARGROUP · ALBORA TECHNOLOGIES · ACLERK DETECTIVES PRIVADOS S.L. · CLOUDFLARE · beazley

CHUBB · HDI · MAPFRE · AVER TECHNOLOGY · everyWAN · NETICS networks & services · IC Hard soluciones en sistemas

Generalitat de Catalunya

Business mapping of cybersecurity in Catalonia: recover segment

Recover

129 companies

Microsoft · Telefónica · T Systems · ORACLE · colt · izertis · sia · NTT DATA · CROWDSTRIKE · axians · abast BUILDING YOUR FUTURE IT · A RICOH Company

accenture · Johnson Controls · it now Experience and Innovation · oesia grupo · S21 SEC Cyber Solutions by Thales · SEIDOR · Atos · dagram · kyndryl · Bitdefender · SERMICRO GROUP digital 40 YEARS · INNOVERY by NEVERHACK

a3kcent · GOVERTIS Part of Telefónica Tech · BECOMIT · NexTReT · A WISE SECURITY · cellnex · basetis · KPMG · Aiuken Cybersecurity · econocom LIVE TECH · build38 · isec auditors

indra · Inycom by nunsys · ‹Avannubo› · getronics · cdmon · claranet · AXA · infoself group · parlem · plain concepts · aggity · quopiam · allento

ITechGrup PLEXUS · cipher a Prosegur company · AETECH · CISCO · ABOX · DETEINCO TICLOGIX · RA Rockwell Automation · IEAISA INGENIERÍA · LIMIT · ToBeIT · HUAWEI · FlexVPC

ALSTOM · Opertek · ITGLOBAL · ADS Anàlisi/Disseny de Soft · asnet · corus · RepScan · trilogi · Adam · OnbrandinG Get back to normal · OnTek · amazon

Quside · ARONTE · pwc · lisot · DLTCode Next Generation Cyber AI · bytemaster · A·D·Q·A · CONTROLIP SERVEIS INFORMATICS · indigo · IBM · nae, · inforxlot

infineon · level4 · grupo paradell Helping Corporations Fight Global Risk · LAN Your Business IT Partner · i2i Solucions tecnològiques · into in · VALORA DATA · TIC SOLUTIONS · Altercom21 · VILAmedi · soctic · esolvo · ESTRATEC 360

infoserveis consultoria informàtica · Partner Gold de: Wolters Kluwer · HITACHI · ene telecomunicaciones · BTIC · ACCON SOFTWARE SUMANDO VALOR · BDR GROUP · ACTUALTIC bringing actual technology since 2013 · GestSoft GW GemWin · LightEyes · laSalle · Verne TECHNOLOGY GROUP · ANIGY · axelia

GRAIL CYBER TECH · numentech · SEVEN SECTOR · SYNERGIAL · Kerberosns Kerberos Network Solutions · asartec · DEKRA 100 YEARS · Orednarbal · aDvens · brontobyte cloud · innovaplanner · IC Hard soluciones en sistemas

OUTLIER CONSULTING · SKY DEVELOPER PROGRAMMER · CCQ Independent IT Care Business Success Stories · GLOFERA. · kipmi On Informàtica Sistemes Solucions · Briko Net Informatica, S.L. · Qualitum · IoT PARTNERS · INDUCONTROL · AVER TECHNOLOGY · everyWAN

Generalitat de Catalunya

Locations of Catalan cybersecurity companies

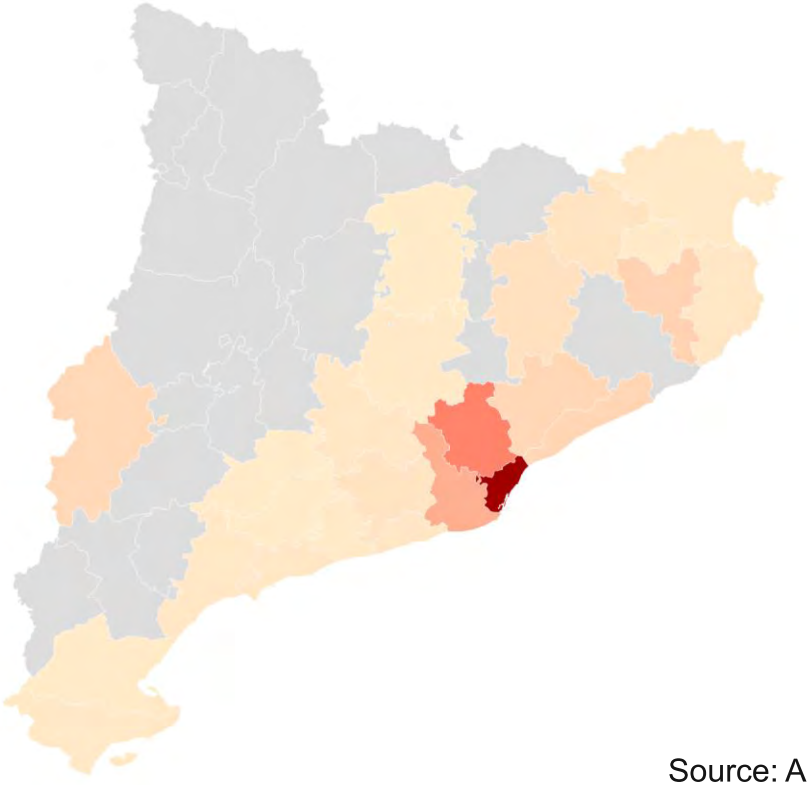
64.7% of the cybersecurity companies are located in the Metropolitan Area of Barcelona (AMB).

The cities include Barcelona (322), Sant Cugat del Vallès (22), Terrassa (15), Lleida (12), L'Hospitalet de Llobregat (11), Sabadell (11), Girona (10) and Cerdanyola del Vallès (9).

County	Number of companies	% of the total
Barcelonès	340	61.0%
Vallès Occidental	69	12.4%
Baix Llobregat	41	7.4%
Gironès	17	3.1%
Vallès Oriental	15	2.7%
Maresme	14	2.5%
Segrià	12	2.2%
Others	49	8.7%
Total	**557**	**100%**

Note: the Metropolitan Area of Barcelona includes 36 municipalities in the counties of Barcelonès, Baix Llobregat, Vallès Occidental and Maresme

Distribution of cybersecurity companies by counties



Source: ACCIÓ

Catalan companies that merge cybersecurity with artificial intelligence

Artificial intelligence

Artificial intelligence is transforming cybersecurity, improving data protection, optimizing algorithms to provide a faster response to threats, and developing solutions to cope with increasingly precise cyberattacks, with Catalan companies at the forefront of this revolution.

238 companies, **42.7%** of the total number of cybersecurity companies

Main applications by segments:

Identify	ANKO	CROWDSTRIKE	NexTReT	Dotpoint	paloalto NETWORKS
Protect	FORTINET	FUJITSU	Mitek	netskope	RED SIFT
Detect	APOLO ANALYTICS	BlackfishID	NeuralTrust	RED POINTS	WISE SECURITY
Respond	asnet	f5	JakinCode	MLCODE	T Systems
Recover	aggity	Bitdefender	build38	NTT DATA	RepScan

Note: partial illustrative image. The companies can be classified in more than one of the segments.

Source: ACCIÓ

Catalan companies that merge cybersecurity with quantum technologies

Quantum technologies

Quantum technologies improve cybersecurity with quantum cryptography, which is practically impenetrable thanks to superposition and quantum entanglement, and help counteract the risks of quantum computing, which could decrypt traditional cryptography, thus guaranteeing data protection in the future.

27 companies, **4.8%** of the total number of cybersecurity companies

Main companies:

cellnex
gmv INNOVATING SOLUTIONS
IBM
KEYSIGHT
LUXQUANTA
oesia grupo
Quside
SATELIOT Space · Connecting · 5G IoT
scAlai UNLOCKING GOALS
sener

Note: partial illustrative image.

Source: ACCIÓ

Agents of the cybersecurity ecosystem

Technological centers and research institutes

BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación
CIT UPC Centre d'Innovació i Tecnologia Universitat Politècnica de Catalunya BarcelonaTech
Crises
Cryptography & Graphs
CSIC
cttc Centre Tecnològic de Telecomunicacions de Catalunya
CVC Centre de Visió per Computador
easy
eurecat Centre Tecnològic de Catalunya
ICFO
IIIA-CSIC Institut d'Investigació en Intel·ligència Artificial
i2cat
inLab FIB
UPC
ISG Information Security Group
IREC
K Cryptography and Information Security for Open Networks
laSalle Universitat Ramon Llull
Parc de Recerca UAB

Undergraduate, master's and postgraduate studies

UPC Universitat Politècnica de Catalunya BarcelonaTech
Universitat Rovira i Virgili
FIB
ENTI
UAB Universitat Autònoma de Barcelona
upf. Universitat Pompeu Fabra Barcelona
Nuclio Digital School
stucom
Institut de Formació Contínua-IL3 Universitat de Barcelona
OBS Business School
Universitat de Girona Fundació UdG: Innovació i Formació
telecos BCN
TecnoCampus
ISG Information Security Group
uic barcelona
Centro de Estudios Garrigues Business & Law School
laSalle Universidad Ramon Llull
UOC Universitat Oberta de Catalunya
Centre d'Estudis Politècnics
IMPELIA Campus Profesional

Vocational programs

Torre Roja Institut
Institut Esteve Terradas i Illa
Institut Caparrella
Institut F. Vidal i Barraquer Tarragona
ICB Institut Camps Blancs
ILERNA
CESF
Institut Pedralbes
Pàlcam
Institut Poblenou Estudis de Comerç, Administració i Informàtica a Barcelona
ENTI
FP llefià
prat
La Salle Manlleu
El Puig
Vedruna Vall Terrassa
Joviat
Institut Badia del Vallès
Institut Carles Vallbona
Insmontsià
bois comp
La Pineda
IFP Innovación en Formación Profesional
FP
Institut de Logística de Barcelona
Institut Montilivi
Linkia FP
Institut Cami de Mar Calafell
Institució Cultural del CIC Fundació Privada
Institut Les Salines
Mundet
Monlau Formació Professional
Lacetània
institut tecnològic barcelona
ites
INS Gabriela Mistral
salesians
Jaume Viladoms Centre Educatiu
Pere Martell
Col·legi Cultural Badalona
Institut de l'Ebre
CampusNET.es
stucom
CIC Cicles Formatius

Associations and events

ISACA Barcelona Chapter
grausTIC
Blockchain
CAES
telecos.cat
Armari
IOT Solutions
NcN
isms forum
OWASP
Barcelona Digital Talent
World Trade Organization
QUANTUMCAT
ITU
aseitec
secpho
APWG
itSMF
ASCICAT
(ISC)²
apep
COETTC-ACETT Col·legi Oficial de Graduats i Enginyers Tècnics de Telecomunicació de Catalunya
COETIC Col·legi Oficial d'Enginyeria Tècnica en Informàtica de Catalunya
MWC Barcelona
Barcelona Cybersecurity Congress
integrated systems europe
Advanced Factories
informàTICa
APCPD
BSides Barcelona

CSIRT/CERT

Agència de Ciberseguretat de Catalunya
ESCERT
a3kcent cybersecurity
LightEyes
CCN-cert
FIRST Improving Security Together
SEIDOR
gmv Innovating Solutions
CSUC
CaixaBank
SFERAIL
incibe-cert_
CSIRT.es
TF-CSIRT Trusted Introducer

Institutions and public administration

Generalitat de Catalunya Departament de la Presidència
Agència de Ciberseguretat de Catalunya
CERCA
AOC Consorci Administració Oberta de Catalunya
incibe_
CCN
ECS
DCA Ciberseguretat
ACCIÓ Catalonia Trade & Investment
Generalitat de Catalunya
DIH4CAT Digital Innovation Hub de Catalunya
enisa European Union Agency for Cybersecurity
apdcat
Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació

Generalitat de Catalunya

Initiatives to promote cybersecurity in Catalonia

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

A body that oversees cybersecurity in Catalonia and ensures a secure digital society for the whole of Catalonia and its public administration.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA | CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

A center whose aim is to promote innovative solutions to improve cybersecurity through the use of functional processes, technologies, knowledge and experience within the Agency's scope of action.

BARCELONA CYBERSECURITY CONGRESS

A three-day event bringing together the main international stakeholders in cybersecurity at a venue for talks and exhibitions.

CYBER[SECURITY]CAT

Catalonia's first cybersecurity research center created by six Catalan public universities with the goal of establishing itself as a center of reference in cybersecurity and privacy research.

DIH4CAT Digital Innovation Hub de Catalunya

A connected network of assets, infrastructures and knowledge in Catalonia geared towards testing and experimenting with advanced digital technologies, including cybersecurity.

DCA Digital Catalonia Alliance

An initiative that brings together six emerging technologies in Catalonia, including cybersecurity, in an alliance of innovative, visionary, disruptive and collaborative technological communities.

ASCICAT ASSOCIACIÓ DE CIBERSEGURETAT DE CATALUNYA

A non-profit organization made up of companies in the value chain of the cybersecurity sector in Catalonia.

Cybersecurity Agency of Catalonia

The Cybersecurity Agency of Catalonia ensures a secure digital society for the whole of Catalonia and its public administration.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

www.ciberseguretat.cat

- The Cybersecurity Agency of Catalonia is responsible for implementing public policies in the field of cybersecurity and developing the cybersecurity strategy of the Generalitat de Catalunya. It is the body that governs cybersecurity in Catalonia.
- The Agency is responsible for establishing the public cybersecurity service and striving to guarantee and increase the level of security of the networks and information systems of Catalonia, as well as the digital trust of citizens.
- As a body competent in the field of cybersecurity, it is tasked with establishing and monitoring cybersecurity-related action programs under the strategic management of the Generalitat de Catalunya, in coordination with the public sector entities of the Administration of the Generalitat de Catalunya and in collaboration with the local governments of Catalonia, the private sector and civil society.

Functions and services

- Cybersecurity governance
- Incident response
- Protection and prevention
- Sensitization

Source: Cybersecurity Agency of Catalonia

Foreign Direct Investment (FDI) in cybersecurity in Catalonia

FDI in cybersecurity in Catalonia has increased exponentially over the last five years, due to the higher degree of digitization caused by the outbreak of the COVID-19 pandemic.

	2015-2019	2020-2024	
Projects	6	**12**	**x2**
Capex (€M)	24	**207**	**x9**
Jobs	267	**976**	**x4**

Companies that have invested over the last five years

netskope · T Systems · Schneider Electric · CROWDSTRIKE · RED SIFT · veriff

getronics · dynatrace · FUJITSU · build38 · relyens · aDvens

Source: the authors, based on fDi Markets

Technological hubs in Catalonia focusing on cybersecurity

160 technological hubs

of foreign companies

+9% compared with the previous year

6,200 new jobs

Economic impact totaling **€2.879 B**

36% of the hubs are dedicated to cybersecurity

Cybersecurity is the **technology with the second-highest degree of implementation in terms of new hubs**, with 29% of the total.

Cybersecurity is **one of the three most popular professional profiles** in the hubs.

Main hubs in Catalonia focusing on cybersecurity:

Boehringer Ingelheim
CISCO
Deloitte.
FUJITSU
getronics
GFT
IBM
KPMG
Lufthansa
Nestlé
NOVARTIS
ORACLE
PEPSICO
Schneider Electric
T Systems
ZURICH

Note: the data refer to 2024.

Source: Mobile World Capital Barcelona, ACCIÓ, Barcelona City Council: “Tech hubs overview”

Catalan cybersecurity research activities at Horizon Europe

15 projects

11.3 million euros

3.2% of the European total

26.1% of the total for the whole of Spain

5th European region in terms of Horizon Europe funding

Horizon Europe

20 institutions

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
eurecat Centre Tecnològic de Catalunya
Applus+ IDIADA
CVC Centre de Visió per Computador
i2cat
FICOSA
BSC
beawre
IREC Catalonia Institute for Energy Research
tttech auto
cttc Centre Tecnològic de Telecomunicacions de Catalunya
FGC Ferrocarrils de la Generalitat de Catalunya
WORLD SENSING
Schneider Electric
IThink UPC

Note: includes Horizon Europe (2022-2024) projects related to cybersecurity (computer security and network security).

Source: Horizon Europe

Cybersecurity talent shortage persists

Need for cybersecurity professionals

According to (ISC)2, the number of cybersecurity professionals has remained stable worldwide, but the labor gap has grown by **19%**, with nearly four million vacancies in the world.

In **Catalonia**, as in Europe, the gap is estimated to have risen by **12.8%**, in such a way that the unmet need for professionals has increased, standing at **13,500** people.

	Existing cybersecurity professionals		Unmet need for professionals	
	vs. 2023	**2024**	**vs. 2023**	**2024**
WORLD	+0.1%	**5.45 M**	+19%	**4.76 M**
EUROPE	-0.7%	**1.3 M**	+12.8%	**392 K**
CATALONIA*	-0.7%	**28 K**	+12.8%	**13.5 K**

**Estimate*

Source: (ISC)2

Training in cybersecurity in Catalonia

45 places of study offer **62** professional training **courses** in cybersecurity

14 master's and postgraduate degrees in cybersecurity

ENTi: Undergraduate degree in Cybersecurity

Institut de Formació Contínua-IL3 Universitat de Barcelona: Master's degree in Cybersecurity Field of the digital transformation

OBS Business School: Master's degree in Business Information Security

uic barcelona: Postgraduate degree in Compliance and Cybersecurity

NUCLIO Digital School: Master's degree in Cybersecurity

telecos BCN: Master's degree in Cybersecurity

UOC Universitat Oberta de Catalunya: Master's degree in Cybersecurity and Privacy

Cybersecurity in networks and systems

Universitat Rovira i Virgili: Master's degree in Computer Security Engineering and Artificial Intelligence

Universitat Politècnica de Catalunya BarcelonaTech: Master's degree in Cybersecurity Management

Master's degree in Machine Learning and Cybersecurity for Internet Connected Systems

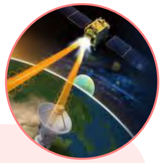
laSalle Universitat Ramon Llull: Master's degree in Cybersecurity

University Master's Degree in Cybersecurity and Critical Infrastructures Management

Quantum initiatives - cybersecurity in Catalonia

Quantum can impact several areas, especially cybersecurity. In Catalonia, initiatives are being conducted to integrate these technologies and reinforce communications security.

QSunset



Quantum key distribution system and entanglement via a low-orbit satellite, including a payload for the satellite and a receiving telescope at the ground station.

6GQuCryptoLab

i2cat 03 23

Installation of I2CAT to simulate point-to-point quantum key distribution (QKD) with trusted nodes, integrating discrete variable (DV) and continuous variable (CV) protocols and satellite network scenarios.

Qspace

Infrastructure to develop quantum key distribution and entanglement via satellite, focusing on nanosatellites and LEO with a quantum payload and 5G/6G services.

Quantum cryptography roadmap

The Generalitat de Catalunya is promoting a €2 M project to prepare for the transition to quantum cryptography in its ICT solutions. The project includes monitoring systems and creating regulations for quantum cryptography.

Qollserola

A cybersecurity ring featuring quantum key distribution (QKD) around the Barcelona metropolitan area.

ICFO cellnex Quside LUXQUANTA

Node Barcelona - Q-Network

EuroQCI

The European Commission and the European Space Agency are promoting EuroQCI, a European quantum communication network with terrestrial and spatial elements. Nodes will initially be created in cities such as Barcelona, which will be connected to each other in a second phase.

EUROQCI SPAIN ICFO cellnex

Source: ACCIÓ

8. Success stories in Catalonia

Business success stories in cybersecurity

BRONTOBYTE is a company specializing in the protection of critical data and business continuity, thanks to its immutable backup platforms and Disaster Recovery as a Service (DRaaS).

ZYNAP is a company specializing in critical data protection solutions and operational assurance for companies.

SONICWALL helps create, scale and manage security in any combination of traditional, hybrid and cloud environments, thanks to its next-generation firewall platform.

SECRETS VAULT has developed a tool that can protect and share sensitive information through the use of images rather than traditional passwords.

QUSIDE is a quantum technology company specialized in the generation, monitoring and processing of randomness, with applications in cybersecurity and high-performance computing.

ZEROD offers a marketplace with ethical hackers from around the world that provide their cyber and advisory services for companies.

NEURALTRUST provides a platform that detects vulnerabilities, blocks attacks, monitors performance, and ensures regulatory compliance for generative AI applications.

WISE SECURITY provides a catalog of cybersecurity services ranging from blockchain technology and offensive cybersecurity to electronic signatures and the management of software vulnerabilities.

LUXQUANTA offers cybersecurity solutions based on quantum cryptography. The quantum signal transmitted via optical fiber generates secure cryptographic keys according to quantum physics.

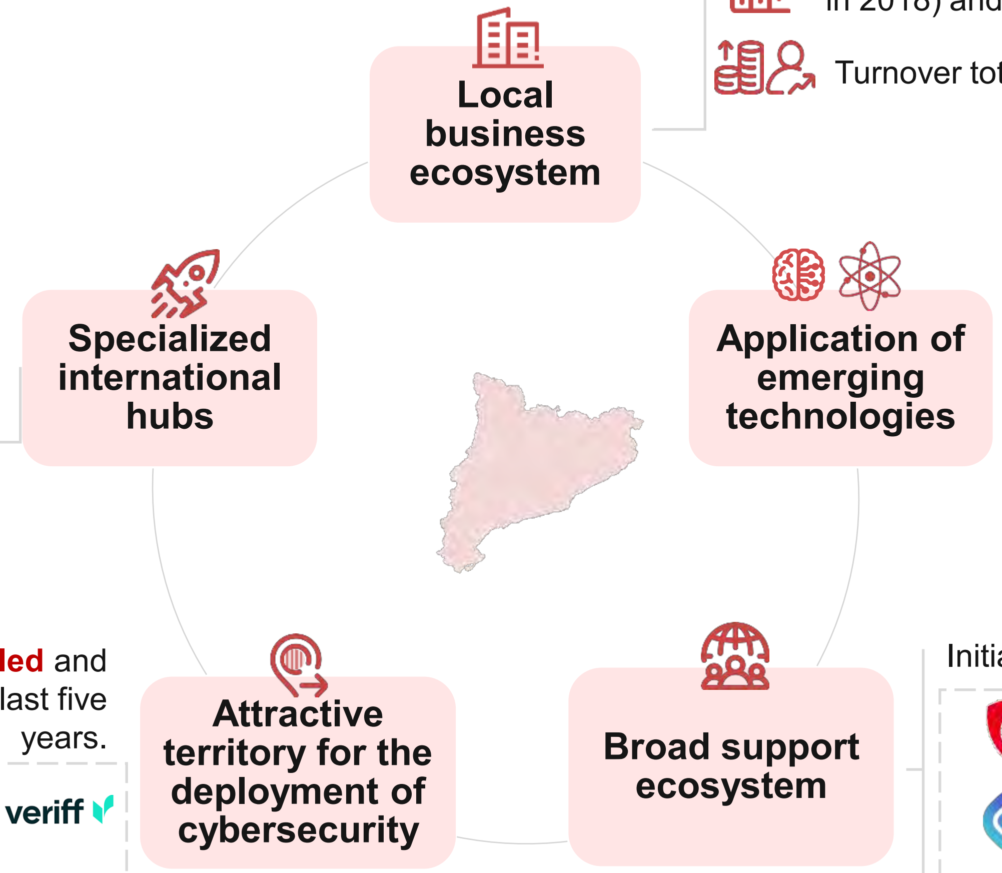
MITEK SYSTEMS specializes in technological solutions to verify digital identities and the veracity of documents, using artificial intelligence, biometric analysis, computer vision, and deep learning.

Catalonia, a dynamic cybersecurity ecosystem

36% of the 160 technological hubs of international companies based in Catalonia focus on cybersecurity.

Cybersecurity is one of the **three most popular professional profiles**.

Boehringer Ingelheim · cisco · Deloitte. · FUJITSU · getronics · GFT · IBM · KPMG · Lufthansa · Nestlé · NOVARTIS · ORACLE · PEPSICO · Schneider Electric · T Systems · ZURICH



Local business ecosystem

Specialized international hubs

Application of emerging technologies

Attractive territory for the deployment of cybersecurity

Broad support ecosystem

557 companies dedicated to cybersecurity (**58.2%** more than in 2018) and **7.9%** annual growth.

Turnover totaling **€1,473 M** (+18.4 %) and **10,672 jobs** (+12.8%).

238 companies (42.7%) develop **AI tools** and **27 companies** (4.8%) develop **quantum technologies**.

6 initiatives to promote the deployment of **quantum** linked to **cybersecurity**.

Foreign investment projects have **doubled** and investment has multiplied by **9** over the last five years.

netskope · T Systems · Schneider Electric · CROWDSTRIKE · RED SIFT · veriff · getronics · dynatrace · FUJITSU · build38 · relyens · Devens

Initiatives to promote cybersecurity in Catalonia

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA · AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA – CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT · BARCELONA CYBERSECURITY CONGRESS · CYBER SECURITY CAT · DIH4CAT Digital Innovation Hub de Catalunya · DCA Digital Catalonia Alliance · ASCICAT ASSOCIACIÓ DE CIBERSEGURETAT DE CATALUNYA

Thank you!

ACCIÓ Catalonia Trade & Investment
Generalitat de Catalunya

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat
@Catalonia_TI

/acciocat/
/invest-in-catalonia/

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Carrer de Salvador Espriu, 51
08908 L'Hospitalet de Ll.

ecosistema@ciberseguretat.cat
ciberseguretat.gencat.cat

@ciberseguracat

@ciberseguracat

More information about the sector, news and opportunities:

https://catalonia.com/key-industries-technologies/technologies/cybersecurity-in-catalonia

Generalitat de Catalunya