CISO as a Service

Winfor Business Security's CISOaaS service offers you strategic cybersecurity management as a service, allowing you to protect your business, comply with regulations and make informed decisions without incurring the cost or rigidity of an in-house CISO.

winfor business security

Who we are.

Winfor Systems is a Spanish technology company based in Martorell (Barcelona), specialising in IT and systems. We are part of the **Winfor group**, where we have been helping organisations modernise with secure, efficient solutions tailored to their needs for over 30 years.

We offer cybersecurity, networking, IT systems and cloud services to ensure operational continuity and maximum performance. With agility and a high level of specialisation, we add value through audits, maintenance and infrastructure protection, acting as a technology partner for the growth and security of our customers.

In this context, the CISOaaS model takes on particular relevance as it offers a more flexible and efficient alternative, backed up by recent data that highlights the growing fear, exposure and economic impact of cybersecurity risks, reinforcing its strategic value.

In Spain, the salary of a full-time CISO can vary between

€80,000-€120,000 /year

The cost of global cybercrime reached

10.5 billion USD

in 2025.

60%

of companies in Spain experienced at least one cyberattack in 2025.

6 out of 10 respondents admit to having

limited knowledge

on cybersecurity.

the average perception of the risk of suffering a cyberattack is

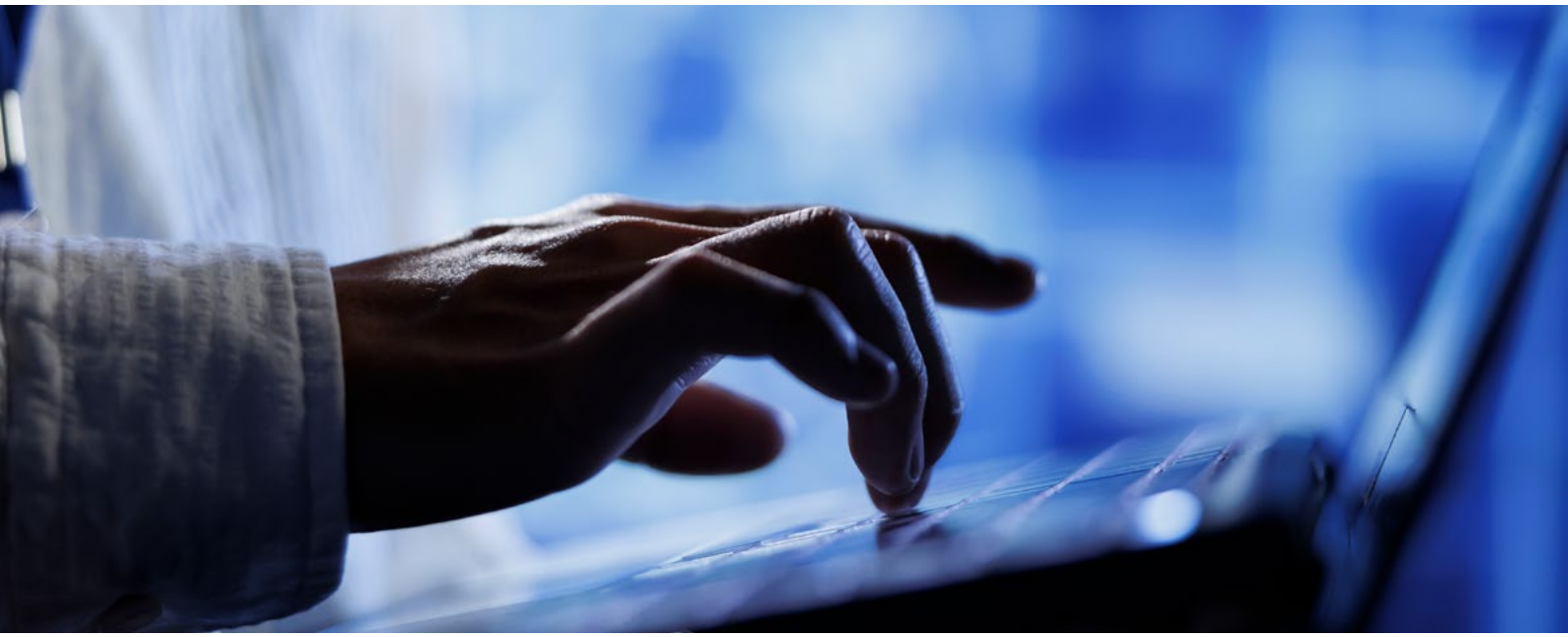
83%

Spain is the

5th country

most affected in the world by cyberattacks.

Winfor Business Security was created as a more cost-effective, flexible security leadership model aimed at minimising business risks.



Our CISOaaS solution offers you greater security, with less complexity and lower costs for your business.

01.
Strategic vision, not just technical expertise

Security aligned with the business, with executive reporting, strategic planning, and rapid incident response.

02.
Flexibility and real scalability

You only pay for what you need: the service adapts to your organisation and evolves according to its growth, security maturity and new requirements.

03.
More affordable costs

You get top-tier security leadership without the cost of a full-time CISO.

04.
Expert team

Immediate access to certified experts with up-to-date experience and high analytical value.

05.
Compliance and reputation

Audits and regulatory advice (ISO 27001, GDPR) that reduce risks and strengthen trust.

Our cybersecurity services.

Vulnerability and exposure analysis

We identify and prioritise the real risks to your organisation, with constant monitoring and support for IT.

· Internal and external vulnerability scans
· Review and validation of technical results
· Prioritisation of mitigations according to business impact
· Ongoing advice to the IT team
· Monthly monitoring with risk evolution

Government and basic security policies

We define the minimum security framework necessary to ensure consistent behaviour aligned with best practices.

· Development and/or review of essential policies
· Secure use of passwords and access control
· Information protection and data management
· Teleworking, mobility and BYOD policies
· Basic incident management procedures

Advanced phishing campaigns

We measure and reinforce awareness levels through realistic simulations.

· Targeted phishing simulations
· Behavioural metrics and risk level
· Training reinforcement after each campaign
· Evolution of the user's level of maturity

Monitoring of action plans

We ensure that the measures defined are implemented and do not remain merely on paper.
· Periodic review of tasks derived from analyses
· Monitoring of technical and organisational mitigations
· Compliance and progress monitoring
· Continuous support

Regulatory compliance and legal advice

We verify minimum and advanced compliance, aligning security and regulation.

· Basic and advanced GDPR compliance checks
· Review of data management and consents
· Privacy policies and information processing
· Advice on ENS and ISO 27001 (if applicable)

Monthly executive meeting

We translate cybersecurity into management language.

· Preparation of executive reports
· Summary of key findings
· Prioritised recommendations
· Brief presentation to management

Technical safety audits

We assess the level of protection of your systems, applications, and networks.

· Wi-Fi network audits
· Code review and secure development processes (SDLC)
· Analysis of web applications and services
· Configuration assessment, hardening, and security controls

Cybersecurity awareness and training

We reduce human risk through practical, ongoing training tailored to the reality of the company.

· Modular cybersecurity courses
· Advice on training plans for employees
· Mini pills with practical advice
· Awareness-raising newsletters and best practices

winfor business security

Our CISOaaS plans.

Not all organisations have the same cybersecurity needs.
But they all need someone to think, decide and lead.
That is why our CISOaaS plans are designed to manage your business security on a global level.

https://winforsystems.com/cisoaas/

CISOaaS Essential
The smart starting point.

CISOaaS Essential is designed for organisations that need to bring order, gain visibility into their risks, and begin to manage their cybersecurity strategy judiciously, without complexity or extra costs.

Essential is control, visibility and support.

Essential

Who is it for?
Organisations that require order, visibility, and basic control:
- Organisations without an internal CISO
- Environments with little security structure
- Need for basic compliance and risk control
- Overloaded or insufficient IT capacity

Benefit
Have a solid foundation of cybersecurity and compliance without complexity or extra costs.

What problems does it solve?
- Lack of clear risk awareness: "we do not know what risks we face"
- Basic regulatory compliance (GDPR, best practices): "We do not have the necessary policies or security framework in place" / "We do not know which regulations we are currently failing to comply with."
- There is no figure who directs business security at a global level.

What is included

01. Initial Security Basic Check.
Initial basic diagnosis:
- Identification of critical assets
- Initial risk and exposure analysis
- Initial executive report

02. CISO Guidance. Monthly support as an external CISO:
- Risk and vulnerability monitoring
- Definition and review of basic security policies
- Advice on essential regulatory compliance (GDPR, best practices)
- Follow-up on agreed actions and improvements
- Phishing campaigns

Additionally, support in employee awareness and training is offered as an extra supplement (not included in the plan).

Advanced CISOaaS
Strategic leadership level.

CISOaaS Advanced offers strategic leadership in cybersecurity for organisations with greater exposure, regulatory pressure or executive reporting requirements.

Advanced is leadership, strategy and decision-making.

Wi** Advanced

Who is it for?
Larger organisations with greater exposure, maturity or regulatory pressure.
- Organisations without an internal CISO
- Environments with little security structure
- Need for basic compliance and risk control
- Overloaded or insufficient IT capacity

Benefit
Strategic cybersecurity management aligned with business, risks, and compliance.

What problems does it solve?
- Growth without risk control: "our risk control has spiralled out of control"
- Regulatory compliance: "We need to have certifications and comply with certain regulations."
- Lack of executive reporting: "we do not know what vulnerabilities or threats we have"
- Reputational and operational risk: "we may lose the trust of our customers and partners", "we have many assets at risk"

What is included

01. Initial Security Deep Check. Initial advanced diagnosis:
- Inventory and advanced classification of critical assets
- Risk analysis aligned with regulatory standards
- Comprehensive report with business impact assessment, cybersecurity maturity roadmap, and quick-win recommendations

02. CISO Leadership.
Advanced monthly support as an external CISO:
- Continuous management of the security strategy
- Progressive development of advanced policies
- Advanced simulation campaigns (phishing, etc.)
- Monitoring of action plans
- Advanced compliance advice (ENS, ISO, etc.)
- Executive reporting and meetings with management

Additionally, support in employee awareness and training is offered as an extra complement (not included in the plan).

Comparison of CISOaaS plans.

	CISOaaS Essential	Advanced CISOaaS
Initial Security Check	Basic	Advanced
Vulnerability analysis and initial report	*	***
Asset inventory and classification	-	*
Strategic roadmap	-	*
CISO management level	Guidance (support)	Leadership
Strategic direction	-	*
Phishing campaigns	*	***
Compliance with security regulations and policies	*	***
Follow-up	*	***
Executive reporting	-	*

"We don't know exactly what risks we face."
We provide you with a clear, prioritised and understandable overview of the status of your cybersecurity.

"We do not have clear policies or a clear security framework."
We lay the foundations for security to begin to be managed in a consistent manner.

Security relies too heavily on IT.
You incorporate a management figure who thinks about security at a global level.

"We have grown, but security has not grown with us."
We define a maturity roadmap aligned with your business reality.

"We need to justify decisions to management or auditors."
We provide executive reporting and ongoing CISO leadership.

Reputational risk is increasing.
We manage cybersecurity as a strategic business asset.

Service guarantees.

Planning

During the planning stage, we efficiently prepare all necessary materials, with a clear focus on:

Identify key data: request only essential data, avoiding both superfluous information and the absence of critical elements.

Anticipate risks and difficulties: identify in advance any potential difficulties arising from the project, the client's organisational culture, the methodologies applied or the tools to be used.

Align expectations with the client: clearly communicate what information and level of involvement will be required, allowing the client to prepare adequately.

Execution

During implementation, the objective is to ensure a smooth experience for the customer, reducing incidents and avoiding unforeseen events by:

Use of proven tools: application of scripts, templates, interview forms, and resources that optimise time and avoid duplication.

Agile incident management: early detection of problems and quick, effective resolution.

Effective and timely execution: carrying out the work in a structured manner, meeting defined milestones and delivering partial results as agreed.

Results

In the final phase, the focus is on maximising the value provided to the customer:

High-quality deliverables: ensuring both the soundness of the content and the clarity and professionalism of the presentation.

Knowledge transfer: ensuring that the client has the necessary knowledge to interpret and take advantage of the results obtained.

Business-oriented approach: all results are presented taking into account the client's needs and their real impact on the organisation.

Certifications.

ISO/IEC 27001 – Information security

National Security Scheme

Information Security Management System ISO 27001 Certified

ens Esquema Nacional de Seguridad

We want to be your partner!

Winfor Systems
Avinguda Sant Antoni
Mª Claret, 6
08670 Martorell - BCN
T. +34 93 749 62 37
https://winforsystems.com/cisoaas/

winfor business security