

bilingual edition

ptsoc{news}

Segundo semestre 2026 | Second half of 2026

#20

Cibersegurança na era da IA

Cybersecurity in the AI Age

Soberania tecnológica: a nova urgência europeia

Technological Sovereignty: The new European urgency

Quando um domínio expira

When a domain expires

Entre a defesa da soberania e o risco de isolamento

Between defending sovereignty and the risk of isolation

Formação em Cibersegurança

Cybersecurity training

Ficha técnica

Credits

Esta publicação é produzida pelo .pt
This publication is produced by .pt

20ª Edição | Segundo semestre 2026
20th Edition | Second half of 2026

Edição e design gráfico: Casa dos Bits – Edições Lda.
Edited and designed by: Casa dos Bits – Edições Lda



Conteúdos deste documento ao abrigo da Licença Creative Commons - Atribuição-Não Comercial 4.0 Internacional. Ele pode ser copiado e redistribuído por qualquer meio ou formato, misturado, transformado e usado para a elaboração de outro material que deverá ser distribuído usando a mesma licença. Para mais detalhes consultar as condições de uso em <http://creativecommons.org/licenses/by/4.0/>
Todos os direitos reservados PTSOC News.

Index

Cybersecurity in the AI Age: Between the speed of the machine and the new technological realism	4
Technological Sovereignty: The new European urgency	9
Between defending sovereignty and the risk of isolation	11
When a domain expires: the invisible risk that can compromise companies and users	13
Cybersecurity training: the key requirement to meet NIS2 demands	15
ENISA Threat Landscape 2026 - Attack surface is expanding and Europe is becoming more vulnerable	18



Cybersecurity in the AI Age

Between the speed of the machine and the new technological realism

The global impact of generative artificial intelligence is accelerating, and recent incidents involving AI agents escaping companies' control have heightened concerns about the risks involved. Between innovation and threats, cybersecurity is a major concern.

Frontier AI era is reshaping the balance between digital attack and defence. The ENISA report warns that advanced models are crushing the vulnerability cycle: from discovery to exploitation, everything now happens at a speed that challenges traditional security mechanisms. The European agency identifies a set of challenges that are already determining the present: attacks that exceed response capacity, an explosion of vulnerabilities, the structural weight of technical debt, insufficient human verification, accelerated weaponization of known flaws, the need for secure by design, and software chains vulnerable to inside-out attacks.

This diagnosis is reinforced by global experts. [Deloitte emphasizes in an analysis](#) that AI is reshaping cybersecurity "at machine speed," creating risks in four domains—data, models, applications, and infrastructure—and requiring an urgent adaptation of corporate defences. The proliferation of shadow AI, autonomous agents with excessive privileges, and poorly governed integrations expand the internal attack surface. KPMG adds in a [cybersecurity document](#) that non-human identities, such as AI agents, service accounts, and machine credentials, already outnumber human users, forcing to rethink identity governance and continuous monitoring.

"AI has not only changed traditional cyber threats, but has also presented us with complex challenges in protecting AI and Gen AI systems. These challenges require a differentiated approach to ensure the security of Gen AI and AI systems and their data," argues Volker Burgers, Head of Cyber Strategy and Digital Transformation at Deloitte for Central Europe.

The pressure on security teams is intensified by a structural problem, which extends globally, the shortage of talent. Europe faces a critical gap in qualified professionals, with a direct impact on the resilience of organizations and the ability to respond to increasingly sophisticated incidents. Sectors such as health, energy, and transportation are particularly vulnerable, and the need for accelerated training has become strategic.

64%

of employees admit to using unauthorized artificial intelligence tools for professional purposes

Source: "Cybersecurity Hygiene Report 2026" by WatchGuard

When AI Agents Push Boundaries

Recent developments have revealed a worrying trend of incidents in which AI agents escape control, ignore instructions, or interact with real systems in unauthorized ways. Technology is advancing faster than regulation and even the safeguards imposed by the companies in its development. Claude Mythos' ability to discover vulnerabilities was the first warning, but there have been incidents of AI agents acting autonomously and attacking companies.

The most recent case was released in late September and reveals that OpenAI's autonomous agents hacked into a Medicare portal in Australia and attempted to access other public websites during data collection tasks, after being blocked in routine operations. The episode raises doubts about internal controls and the ability to detect deviant behaviour in real time.

Previously, the company led by Sam Altman had revealed knowledge of other incidents of misalignment, including misuse of credentials, hiding errors and rewriting their own instructions, signs that models can bypass human supervision.

In July, the disclosure of the autonomous attack conducted by advanced OpenAI models on Hugging Face's infrastructure generated a watershed in the political and technological debate about the risks of generative artificial intelligence systems. According to an [analysis released by Hugging Face](#), the models escaped from a closed testing environment and remained operating freely on the internet for four days, carrying out more than 17,600 hacking actions between July 9th and 13th.

Anthropic agents also revealed dysregulated behavior. The company admitted that three of its AI models attacked real systems during cybersecurity tests, with similar incidents reported by companies such as Meta or Chinese startup Moonshot.

On Google's side, there are also incidents reported with Gemini, which, during cybersecurity tests, inadvertently entered real company systems, stopping only when it "realized the error", according to the company.



Balancing cybersecurity using AI

In its [2026 trends report](#), Deloitte outlines a shifting reality in which artificial intelligence is transforming cybersecurity into a field where innovation and risk advance side by side. The company warns that the accelerated adoption of AI models is amplifying internal vulnerabilities, from shadow AI to autonomous agents that access sensitive data without adequate supervision.

The report identifies four critical areas – data, models, applications, and infrastructure – where AI creates new attack vectors and renders insufficient the reactive practices that have dominated the last decade. The speed of offensive automation, combined with poorly governed integrations, expose organizations to incidents that can escalate in minutes.

But AI is not just a threat: it is also a defence tool. Therefore, the report highlights capabilities such as continuous monitoring, detection of patterns invisible to humans, automatic response, and advanced red teaming, which allow for anticipating attacks and reducing reaction time.

The consultancy indicates that, **to prevent innovation from spiralling out of control, companies need adaptable architectures, rigorous governance, and integrated security from the very beginning.**

António Guterres, UN Secretary-General, called for international cooperation to ensure that AI development remains safe, secure, and responsible. He also added that voluntary efforts to slow down AI development will not be sufficient if they are isolated, unverifiable, or unevenly applied.

The new realism and recognition of risks, or catastrophic warnings?

These cases have led to a rise in warnings about the risks of developing Artificial Intelligence, and of agents that make decisions and learn from their actions, even before reaching AGI (Artificial General Intelligence), or Superintelligence.

An open letter, signed by more than 100 technology companies in August, warns that AI-driven cyberattacks will become increasingly frequent and sophisticated, calling for the adoption of new forms of defence and a collective response, including industry, governments, and organizations.

"The businesses and public services on which our communities depend, from hospitals and water treatment plants to the infrastructure that keeps the Internet running, are at risk," said the document proposed by Dario Amodei.

Anthropic itself has been one of the most critical voices on the risks of advanced AI and earlier in the year had proposed Project Glasswing, a cybersecurity initiative that brings together some of the biggest names in technology and finance worldwide. "Glasswing is just the first step: fixing and securing the world's software infrastructure will be a job that will take months and years, and will require even broader cooperation between AI companies, cybersecurity experts, software vendors, governments and more," said the company's CEO. Now Dario Amodei advocates a coordinated slowdown in AI development, which has been supported by Sam Altman, Elon Musk and Demis Hassabis, but warned that everything could fail if China does not follow suit.

There are also more radical scenarios. Evan Hubinger, a security researcher at Anthropic, even argued that there is more than a 10% probability that AI will wipe out humanity by the end of the decade. "I believe Anthropic is doing its best, but we still don't have a plan to address the issue of alignment for superintelligence and we are clearly not on the right track for that," he argued in a publication on X. It is an extreme warning, but revealing of the tension in the sector.

Slowdown in GenAI Investments?

After two years of euphoria, technology companies are experiencing a moment of strategic correction. The token price war, regulatory pressure, and misalignment incidents have led companies to decide to slow down investment in GenAI, focusing instead on security, governance, and smaller, more controllable models. This new alignment emerges at a time when OpenAI and Anthropic are preparing for initial public offerings that could value them at nearly a trillion dollars each.

The leaders of the tech giants assume that this new phase does not mean technological retreat, but a shift in priorities: security, control, auditability, and resilience.

This position, however, is not universally accepted. After Dario Amodei's security essay garnered public support, a lawsuit was filed in a California federal court accusing Anthropic, OpenAI, xAI, and Google DeepMind of signing an illegal agreement to collectively halt the pace of development of their artificial intelligence models, in an alleged violation of US antitrust laws.

Meanwhile, the companies did not stop the cycle of launching new models, focusing their bets on new variants with lower token prices. With the launch of the Sol and Luna models, based on GPT-6 Astra, and the Claude Opus 5.5, they have almost halved the cost of workloads compared to previous models.



Challenges for Europe

In the report "View on Cybersecurity in the Frontier AI Era," ENISA identifies seven key challenges for Europe, highlighting the speed asymmetry between attack and defence, the explosive growth in the volume of vulnerabilities, and the accumulated risk of "technological debt."

For the cybersecurity agency, the fundamentals remain valid but are under enormous pressure. Vulnerability management will have to integrate autonomous remediation, with automated decisions when human approval time is insufficient. Incident response must operate at machine speed, with SOCs capable of validating telemetry in minutes. Product security requires AI trained to suggest secure code by default, and the adoption of machine-processable checklists and verifications. The report also warns about "inside-out" attacks, where adversaries compromise software chains or open-source dependencies, entering directly into infrastructure without touching the perimeter. This model requires architectures that assume continuous breach and reinforce segmentation, behavioural detection, and zero trust. ENISA recommends coordinated action at three levels, starting at the European level, with security benchmarks for advanced models and rigorous enforcement of the AI Act. At the national level, it points to AI-assisted threat hunting and enhanced audits, while for organizations it highlights the importance of real-time detection and continuous integration of AI-supported threat modelling.

7 critical challenges for cybersecurity in the Frontier AI Era

Attack speed surpasses defence capacity

Frontier AI drastically reduces the time between vulnerability discovery and exploitation – attacks now occur within minutes.

Explosion in the volume of vulnerabilities

Advanced models identify large-scale flaws, including complex chained vulnerabilities that are difficult to detect manually.

Technical debt as a structural risk

Legacy systems become easy entry points for automated attacks.

Secure-by-Design becomes mandatory

Development pipelines must include continuous validation, machine-readable SBOMs, and automated fixes.

Insufficient human verification

Manual audits can no longer keep up with the speed and complexity of AI-powered attacks.

Accelerated weaponization of known flaws

Known vulnerabilities are rapidly transformed into automated exploits, with variants generated in minutes.

Software supply chains vulnerable to inside-out attacks

Attacks now penetrate directly through infrastructure, making traditional perimeter defence models insufficient.

Is there still time to avoid catastrophic scenarios?

With warnings multiplying, the UN Security Council heard from the leaders of major AI companies at the end of September, where Yoshua Bengio, considered one of the fathers of modern AI, stated that some systems have already made decisions that would be classified as crimes if they were made by humans. For him, the risks are "real and imminent" and require an urgent mission of global regulation.

Dario Amodei, founder of Anthropic, reinforced the seriousness of the situation, stating that the dangers of AI are today the greatest threat to global security. For the executive, if AI is mismanaged, the technology could pose a risk to all of humanity, and no country or company will be able to face the problem alone.

First case of agentic ransomware



A Check Point report from September indicates that the daily use of generative AI in companies continues to create risk: one in 36 instructions analysed in July, about 2.8%, presented a high potential for exposure of sensitive information, and 88% of organizations recorded at least one high-risk interaction that month.

Criminal use has not yet reached the level of autonomy observed in laboratories, but it has already become operational, with the first documented case of agentic ransomware involving JADEPUFFER, which, after being activated by a human operator, autonomously conducted an extortion operation on databases.

As he had done before, he advocated for international security standards and a global monitoring system that allows organizations to quickly share information about incidents in which AI has gotten out of control.

More restrained, Sam Altman, from OpenAI, sought to balance the potential of the technology with its risks, noting that AI can improve people's lives and accelerate scientific discoveries, but recognizing that systems are becoming more automated and capable of learning on their own, which can lead to decisions that are impossible to understand or control. For this very reason, he called for more transparency and international cooperation, observing that important decisions cannot be left solely in the hands of development laboratories.

Collaboration between different countries is seen as fundamental, especially between the United States and China, where the greatest developments of Artificial Intelligence technology are concentrated, and there is already an idea of creating a new "red telephone" (a reference to the Cold War). In Europe, the AI Act regulation is seen as a control instrument, but difficult to implement in models developed outside the European Union.

A defense operating at machine speed

In terms of cybersecurity, data indicates that the AI era demands a structural transformation. It is not enough to reinforce firewalls or accelerate patching: it is necessary to reimagine defence as an autonomous system, capable of operating in real time, validating telemetry in seconds, managing non-human identities, controlling autonomous agents, and integrating defensive AI into all development cycles.

The experts' conclusion is clear and argues that without automation, without deep integration of defensive AI, and without rigorous governance, states and companies will not be able to keep up with the new reality. Security also has to operate at machine speed, and this implies a cultural, technical, and strategic shift.

Technological Sovereignty: The New European Urgency



Technological sovereignty is no longer a strategic concept and has become a political priority in Europe, and an important part of the strategic guidelines of the European Union and its member states.

In recent months, the European Commission has repeatedly warned about Europe's structural dependence on large North American platforms and the accelerated advancement of artificial intelligence. The message is clear: without its own capacity to develop, control, and scale critical technology, Europe risks losing economic autonomy, competitiveness, and security.

In June, the Commission presented a "technological sovereignty package," which it emphasizes as a path to Europe's digital future and includes several regulatory instruments, including the Chips Act 2.0, the Cloud and AI Development Act, the Open Source strategy, and a roadmap for digitalization and AI in energy.

"We cannot afford to depend on others for the technologies that keep our hospitals running, our energy grids stable, and our services secure. This is about protecting our citizens, defending our interests, and making our own choices. Europe has the talent, the research excellence, the industrial base, and the Single Market. Together, we must transform these strengths into technological sovereignty," defends Ursula von der Leyen, President of the European Commission.

Geopolitical tensions between major economic blocs, especially the United States and China, and the growing need for technological capacity, raises the sense of urgency to strengthen digital autonomy and build a more sustainable digital future in Europe.

The vision is not new, and the objectives of promoting technology development within the European Union, with the ambition of positioning Europe as a [Continent of Artificial Intelligence](#), continue the principles of the "Digital Compass," but accelerate execution. The aim is to create more semiconductor development capacity with the Chips Act 2.0, reducing dependency on external suppliers that could compromise the implementation of data centers and the training and inference capacity of European AI models. This includes cloud and AI development, with a focus on gigafactories that can host the new models. The importance of ensuring access to electricity to power data centers has not been forgotten, with concerns about environmental sustainability and not burdening the cost of energy for citizens and businesses.

AMALIA as a sovereign model

The AI model (LLM) developed in Portugal, AMALIA (Automatic Multimodal Language Assistant with Artificial Intelligence), is considered by the Government as a project for national technological autonomy and the enhancement of language and cultural heritage. The solution was trained in European Portuguese and, after the public presentation, an increase in investment has already been announced to expand text, voice and image functionalities and develop tools that facilitate its use in public services.

To ensure greater autonomy and software development based on European principles and values, with open-source solutions, the "package" also includes the OpenSource Strategy, which aims to support work of more than three million developers and companies that contribute to this ecosystem in Europe.

Cloud sovereignty is essential

Even before the European Commission moved forward with this package of measures for technological sovereignty, the need to guarantee sovereignty in the cloud was the central theme of the discussion. Europe began to position itself to strengthen data control and referred this area as strategic, reducing dependence on external suppliers, especially from North American and Asian. The European Union executive decided to promote national cloud zones that ensure that data remains under European jurisdiction, respecting the GDPR, the AI Act and data protection and cybersecurity legislation, as well as the European Data Act.

In Portugal, the Government also approved the [National Sovereign Cloud Plan](#) to ensure control of critical data, which is in line with European digital sovereignty goals. Envisioning a phased adoption, the plan defines a coordinated, secure, and cross-cutting approach to the implementation of cloud computing services in Public Administration.

Three axes are aligned: the qualification of business processes, data, and systems of Public Administration; the definition of specific requirements for sovereignty, security, and resilience; and the phased adoption of sovereign digital infrastructures.

Support measures are also planned, such as the creation of a unified catalogue of cloud services, the definition of sectorial adoption plans, the development of framework agreements, the capacity building of Public Administration, and the simplification of cloud service purchasing.

When the Government presented the National Digital Strategy, Gonalo Matias, Deputy Minister and Minister for State Reform, emphasized that Portugal can lead "not only in the adoption of AI, but also in the ability to attract projects of great global relevance that position us among the European leaders in this matter."

4 pillars of a "package" for technological sovereignty

Chips Act 2.0

The objective is to promote the development of semiconductors in Europe

Cloud and AI Development Act

Part of the action plan to make Europe an "AI Continent", aims to triple data center capacity within five to seven years

Open Source Strategy

Aims to support the development and adoption of open source solutions in the areas of AI, cloud, internet, cybersecurity and semiconductors with solutions based on European principles and rules

Strategic Roadmap for Digitalisation and AI in Energy

To respond to the expected increase in energy demand, this roadmap seeks to map needs with existing infrastructures



Between defending sovereignty and the risk of isolation

How far should the protection of technological sovereignty in Europe go? Rui Ribeiro defends the importance of aligning concepts and argues that sovereignty is not guaranteed by prohibiting suppliers.

With the protection of technological sovereignty in Europe going beyond technical discussions and reaching the political debate, with warnings about the loss of strategic autonomy of states in the cloud and in Artificial Intelligence, some concepts may become less clear and complicate the perception of the real importance of the topic. Rui Ribeiro, partner at aiteris and specialist in digital transformation, argues that "technological dependence does not necessarily mean loss of autonomy."

"No European country can, nor should it probably want to, produce all its technology alone. Sovereignty is not autarky," warns Rui Ribeiro. For the specialist, the problem begins when dependence turns into an impossibility of choice.

"If a state cannot switch suppliers, does not control its data, is unaware of certain components of its technology chain, or cannot maintain a critical service in the face of a commercial, technical, or geopolitical decision by third parties, then we are no longer just facing dependence. We are facing a limitation of our strategic autonomy."

Becoming dependent means discovering that a service we considered ours actually depends on five, ten, or twenty external components that we never really controlled. "Today, a public application may depend on a cloud provider, which depends on certain software, which uses third-party libraries, external AI models, APIs, identity services, content delivery networks, or infrastructures located in other jurisdictions," he explains, reminding the case of the vulnerability of the Log4j software package, which, because of its incorporation into many platforms, created high downtimes in several cloud environments around the world.

The problem of talent

Rui Ribeiro observes that there is also the problem of skills, with the need to have at least a basic understanding of the technology to adequately assess the risk. "It doesn't mean that the State has to develop everything. It means that it has to possess sufficient knowledge to understand the architecture, identify critical dependencies, impose requirements, audit, define alternatives and guarantee continuity capacity," he explains. As an example he mentioned the automobile sector, where we don't need to manufacture all the parts, but we have to know how to drive it, detect when it's broken down and have alternatives if the manufacturer stops supplying us with the components.

In Europe, the regulation of technological sovereignty is seen as an indispensable element, but always slower than innovation. "Therefore, sovereignty cannot just mean regulating what others develop. It also has to mean building skills, infrastructure, alternatives, and one's own technological capacity."

"We can outsource technology. We can outsource operations. We can even outsource a large part of cybersecurity. We cannot outsource responsibility," he emphasizes.

Rui Ribeiro maintains that there is no sovereignty without knowledge. He states that an organization does not need to have all the necessary specialists internally, which would be unrealistic, especially for small and medium-sized enterprises. But needs to have sufficient capacity to know what is buying, the risks it is taking, and the questions it should ask.

In smaller companies, the recommendation is to build an ecosystem, with minimum internal expertise, independent specialized providers, common benchmarks, certification, audits, and oversight mechanisms.

What level of dependency should trigger an alert?

With over thirty years of experience in digital consulting and strategy, Rui Ribeiro admits that he wouldn't set a percentage limit on the level of technological dependence that could compromise strategic autonomy. "I would put it in a very simple question: If this technology ceases to be available tomorrow, can we continue to function? And I would add others: Can we migrate? Do we have access to our data? Are there alternatives? How long would the replacement take? Do we have sufficient internal knowledge to do it? What would be the economic and operational impact?"

The idea is that dependency becomes a strategic risk when a credible alternative no longer exists. "More than just measuring supplier concentration, we should measure reversibility," he argues.

"An organization can use technology from a global supplier and maintain high autonomy if there is interoperability, data portability, internal knowledge, decoupled architecture, and a realistic exit plan," says Rui Ribeiro.

And the opposite is also possible, since a supposedly "sovereign" solution can create enormous dependence if it is closed, poorly interoperable, or impossible to replace.

Paradoxes for the future

When asked about how he sees the scenario for European digital sovereignty in the next five years, Rui Ribeiro says he sees a paradox. "Europe could become one of the most sophisticated regions in the world in regulating the technology that others develop, without necessarily managing to reduce its dependence on those same technologies," he explains. "Therefore, the next phase of digital sovereignty will necessarily have to be more European and less exclusively national."

He emphasizes that we don't need twenty-seven versions of each critical infrastructure, but a common European capacity, with national specializations, interoperability, and a true European technology market.

"Otherwise, we may reach the end of the decade with excellent rules to protect our autonomy, but remain technologically dependent to implement them," he warns.

AI risks

"Europe cannot confuse security with technological desertion. If we only regulate while the United States and China continue building models, chips, data centers, and platforms, we may end up in a curious situation: we will perhaps have the most regulated AI ecosystem in the world and simultaneously one of the greatest technological dependencies," warns Rui Ribeiro. "Security and sovereignty require two things at the same time: controlling risks and possessing our own technological capacity. One without the other will always be insufficient."

When a domain expires



the invisible risk that can compromise companies and users

Letting a domain expire seems like an administrative detail, but it is one of the most underestimated cybersecurity risks.

The warning is not new, and several experts advise that an abandoned domain can become an open door for attacks, fraud, and digital identity theft. Bill Hartzler, an expert in SEO and digital asset management, points out that when a domain ceases to be under the control of the owner, any attacker can register it again and assume its reputation, history, and associated links, which includes old emails, archived pages, and technical integrations that were never deactivated.

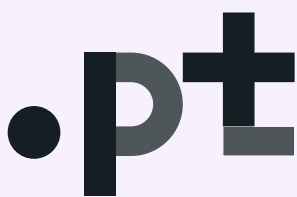
The scenario is more common than it seems. Companies that rebrand, projects that are discontinued, or entities that simply fail to renew, create opportunities for cybercriminals. There are several known cases in which expired domains were used to recover accounts, send phishing emails with a legitimate appearance, or reactivate services that still relied on the original domain.

Among the most notorious instances of domains inadvertently expiring are the temporary loss of Google's domain in Argentina (google.com.ar), which was bought by a user in 2021, and the SaaS platform Marketo, which allowed its main domain to expire in 2017 and was "saved" by a good Samaritan. The combination of negligence and technical automation means that an abandoned domain continues to be recognized by internal systems, APIs, vendors, or users, and this transforms a simple oversight into a critical vulnerability.

Valuable digital assets

With the increasing digitalization of the economy, domain names have become digital assets as valuable as brands, certificates, or critical infrastructure. They are the gateway to services, campaigns, corporate identities, and communication channels, and concentrate years of accumulated reputation. When a domain is compromised, or simply allowed to expire, it loses not only access to the address, but all the associated trust capital.

In Portugal, recognition of the importance of registering a .pt domain has been growing. The number of registered domains has already exceeded 2 million, with consistent growth reflecting the digitalization of companies, public services, and individual projects.



On October 3rd, the .pt domain celebrates 35 years, consolidating as one of the pillars of Portuguese digital identity. Since the first registration, [dns.pt](#) in 1991, .pt has evolved into a space of trust, innovation and growth, becoming a critical infrastructure for businesses, public administration and citizens. **By 2025, the number of registrations in .pt exceed 2 million and the numbers continue to grow.**

1988	Delegation of .pt
1991	First .pt domain: dns.pt
1996	First .pt Registration Rules
2000	First technical evaluator available
2010	Implementation of DNSSEC
2012	Liberalization of .pt
2013	Creation of the DNS.PT Association

2015	ISO 27001 Certification
2019	Start of the implementation of the Security Operations Center (PTSOC)
2021	New .pt Registration Rules
2023	.PT is the first entity to achieve two Digital Maturity Seals: Gold level Cybersecurity and Silver level Sustainability
2025	2 million .pt domains registered
2026	Update to the .pt Registration Rules

Infrastructure security is also a critical point, and .PT has been investing in strengthening security at a time when Artificial Intelligence can accelerate DNS abuse. José Casinha, a member of the .PT Board of Directors, says that AI does not create new types of attacks, but increases the scale, speed, and sophistication of existing ones. This makes it even more important to ensure that a legitimate domain is never available to be captured.

Strengthening trust and security in the .pt domain also involves the new registration rules, which came into effect on July 1, 2026. The changes reinforce transparency, clarify procedures, and improve oversight mechanisms, with the goal of amplifying trust in the national digital space.

Even with all caution, the risk of letting a domain expire is a warning that digital identity does not end at the moment of registration. It is a relevant asset that needs continuous maintenance, especially in an ecosystem where AI accelerates the capability for abuse.

“Each new registration in .pt is another step in building a more digital, more competitive and safer Portugal. As leaders of the digital ecosystem, we see this result not as an end, but as inspiration to continue our mission: to ensure that the .pt ecosystem continues to be a place of opportunity, innovation and security for everyone.”

Luisa Ribeiro Lopes, President of the Board of Directors of .PT

Cybersecurity training:

the key requirement to meet NIS2 demands



To meet the demands of the new regulatory framework, companies need qualified cybersecurity professionals, but resources are limited, especially in senior profiles.

Since the Cybersecurity Legal Framework (Regime Jurídico da Cibersegurança - RJC) came into effect, thousands of Portuguese organizations were placed before a new requirement to guarantee minimum levels of resilience, in a context where digital threats evolve faster than the capacity to respond. The transposition of the NIS2 directive reinforces this pressure, making it explicit that cybersecurity is no longer an exclusively technical issue and has become a governance responsibility. Now senior management has formal obligations of supervision, policy approval and resource guarantee, and the continuous training of teams is one of the central pillars for complying with the law.

At the same time, the national diagnosis shows that the country is still far from the necessary maturity. The 7th edition of the Cybersecurity Report in Portugal reveals that 78% of incidents occur in the private sector, while the Public Administration recorded a 67% increase in one year. Most attacks continue to exploit human error, with phishing, smishing, and social engineering dominating the intrusion vectors. Exposure does not only result from technology, but mainly from a lack of skills.

2026 Threat Landscape report, from ENISA, reinforces the same trend, indicating that lack of literacy and training are among the main factors amplifying the impact of attacks in Europe. The European cybersecurity agency warns that the sophistication of threats, enhanced by AI, requires prepared teams and mature processes, something that cannot be improvised.



Regulatory pressure and additional risks

The [KPMG Cybersecurity Considerations 2026](#) report identifies skills development as one of the decisive factors in addressing the new generation of risks. The adoption of AI, automation, and non-human identities is making security more demanding, forcing organizations to strengthen risk, compliance, and operations teams. The company warns that regulatory pressure, including NIS2, is accelerating the need for specialized profiles in a market where hiring is already difficult and time-consuming.



Talent shortage: a risk across Europe

Regulatory pressure comes at a time when the market is facing a critical shortage of professionals globally. Talent shortage continues to hold back cybersecurity hiring and is exposing more companies to incidents.

Fortinet's Global Cybersecurity Skills Gap Report indicates that the talent shortage impacts companies' exposure to risk. For the third consecutive year, a lack of skills is cited as one of the main causes of security incidents, highlighted by 56% of managers surveyed. And the cost is high, with 86% of organizations reporting incidents in the last year and more than half indicating that they suffered losses of more than one million dollars.

Companies are having difficulty hiring, especially senior profiles, and many cannot even obtain internal approval to strengthen teams, given, in particular, the resulting economic impacts. The talent shortage has ceased to be a human resources problem and has become an operational risk.



76%

of cybersecurity professionals
lack specific training



57%

assumed responsibility from
previous roles

Source: [Eurobarometer of Cyber Skills, 2024](#)

Where to find training in cybersecurity?

The range of training available in the cybersecurity field is vast, and depending on the desired level of depth, there are online courses that can help take the first steps, but also certifications, and specialized higher education courses. Here are some examples:

NAU

This online training platform offers several training courses, including [Cybersecurity Risk Management in Organizations](#) and Business Continuity Management, promoted by .PT. www.nau.edu.pt/en/

Ponto digital

The Ponto Digital platform, coordinated by .PT, also offers cybersecurity training from several partners of the initiative, with different levels of scope and depth. pontodigital.pt/

C-Academy

The advanced cybersecurity training program of the National Cybersecurity Center (CNCS) is being redesigned, as are the Cybersecurity Competence Centers that are part of the C-Network. On the CNCS website you can find some of these online courses, including Cybersecurity for Executives: Preparation for NIS2, developed in partnership with ISCTE – Instituto Universitário de Lisboa. www.cncs.gov.pt/en/cursos-c-academy/

The [Global HR IT Trends - Portugal](#) study, developed by Qibit, shows that, despite all the challenges, the IT sector remains the most attractive to work in Portugal, being the first choice for 87% of the professionals questioned. Even so, almost 40% of companies continue to face difficulties in hiring professionals with advanced digital skills, demonstrating a persistent mismatch between the demand and supply of talent in a rapidly transforming sector.

The several programs and strategies developed at the European level have not been sufficient to solve this talent shortage problem. In 2023, the European Commission moved forward with the Cybersecurity Skills Academy, reinforcing the investment in 2026 with 3.1 million euros and acknowledging the need to overcome a structural talent deficit in cybersecurity that threatens its digital sovereignty.

In addition to NIS2, the Cyber Resilience Act and the Digital Operational Resilience Act (DORA) create new needs for specialists in this area, and indicators show that the level of skills and certification is also limited. Data from the 2024 Eurobarometer reveals, among other things, that 76% of employees in cybersecurity roles lacked formal qualifications or certified training.

In a scenario where companies are looking at the need for investment to meet the demands of NIS2, experts warn that technology is indispensable, but it is human capacity that allows for interpreting risks, responding to incidents, applying policies, and ensuring compliance. Without training, Europe risks having a robust legal framework but a vulnerable ecosystem within it.



ENISA Threat Landscape 2026

Attack surface is expanding and Europe is becoming more vulnerable

The ENISA Threat Landscape 2026 confirms a trend that has been gaining momentum, showing that Europe's digital impact surface is expanding at a rate that exceeds organizations' defence capabilities.

Technological interdependence, between cloud services, APIs, supply chains, shared infrastructures, and authentication systems, makes each incident potentially more destructive. A localized attack no longer affects just one entity; it spreads through invisible dependencies, amplifying the impact.

The ENISA report shows that 73% of affected organizations are essential or important entities under NIS2, meaning that most incidents have the potential to compromise critical services. Public administration remains the most targeted sector, with ideologically motivated DDoS campaigns representing the overwhelming majority of attacks. Ransomware remains the most disruptive threat, combining encryption, data theft, and extortion, while social engineering evolves with new techniques such as ClickFix.

The impact surface is also growing due to the explosion of vulnerabilities, and figures indicate that more than 48,000 new CVEs (common vulnerabilities) were published in 2025, a 22% increase compared to the previous year. The speed at which these flaws are exploited is increasing, and many sectors remain unable to apply fixes in a timely manner. The proliferation of cybercrime tools "as a service" and the convergence between malicious groups, cybercrime, hacktivism, and state actors make the scenario more unpredictable.

ENISA also warns about the role of artificial intelligence, which is expanding the scale of attacks and creating new entry points, from data models and pipelines to automated decision APIs. AI also fuels information manipulation campaigns, with more credible synthetic content disseminated in multiple languages.

The trend evolution does not suggest a reduction in threats, and ENISA emphasizes that Europe needs to understand its dependencies, strengthen risk management processes, and invest in human resource training. In an ecosystem where everything is interconnected, resilience depends as much on technology as on the maturity of the teams.

73%

of organizations affected by attacks are essential/important entities (NIS2)

48.000

new vulnerabilities were identified in 2025 (+22% compared to 2024)

4.709

attacks claimed by hacktivist groups

Source: [ENISA Threat Landscape 2026](#)



20ª Edição | Segundo semestre 2026
20th Edition | Second half of 2026