devoteam
Cyber Trust

Opinion Article

Opinion article published in SAPO Tek, a Portuguese technology news website.

When resilience becomes structure

For years, cybersecurity was treated by organisations as an add-on, a kind of reactive mechanism, almost decorative, installed at the last minute to protect a building that had already been erected. It was the equivalent of placing an alarm system in a structure that was never designed to withstand threats. However, with the entry into force of Decree-Law No. 125/2025 on 3 April 2026, that paradigm no longer makes any sense.

This new legal framework, which transposes the European NIS 2 Directive into national law, marks a profound shift: digital security ceases to be a technical detail and instead becomes one of the structural pillars of any organisation. Just as a building cannot be constructed without an approved structural design, it is no longer acceptable to operate without a robust digital resilience strategy. Portugal thus enters a new era, one in which security is mandatory, transversal, and inseparable from the organisation's operations.

One of the most significant transformations introduced by this legislation is the central role assigned to leadership. Cybersecurity is no longer confined to technical teams; it becomes a direct responsibility of governing bodies. The notion that "the example comes from the top" now carries the force of law. Executives are no longer mere observers of technological decisions; they are active agents responsible for their organisation's resilience.

This entails, first and foremost, the formal approval of risk management measures, ensuring that the "blueprint" for security is properly designed and validated. It also requires investment in internal capacity-building, ensuring that everyone, including leadership itself, has sufficient training to recognise vulnerabilities and act preventively. More than that, it demands accountability: members of governing bodies may be held personally liable for serious failures, whether by action or omission. Signatures are no longer symbolic; they are binding.

But this transformation does not stop at the top. The scope of entities covered is also significantly expanded. Whereas in the past only traditionally critical sectors, such as energy or banking, were subject to strict scrutiny, the perimeter now includes areas such as waste management, wastewater, manufacturing, and the food sector. This expansion is not arbitrary; it reflects the reality of a deeply interconnected economy, where an apparently isolated failure can trigger cascading effects with national impact.

In this context, a particularly demanding new challenge emerges: supply chain security. It is not enough for an organisation to be robust internally if its suppliers represent vulnerabilities. Just as a building cannot withstand pressure if constructed with poor-quality materials, an organisation cannot be resilient if it depends on fragile partners. The decree-law therefore requires a shift in approach: suppliers are no longer a secondary variable but an integral part of the security strategy.

This translates into the need for stricter selection criteria, including prior assessment of the cybersecurity maturity of partners and service providers. It also requires a careful review of contracts, ensuring they include clear clauses on security, service continuity, and incident response, particularly in contexts such as cloud services or critical software.

To support this new framework, the National Cybersecurity Centre provides the MyCiber platform, which serves as a central point of coordination between organisations and authorities. More than a technical tool, it functions as a genuine control panel for the regime, enabling entities to understand their legal standing and fulfil their obligations in a structured way.

It is important, however, not to reduce this shift to a matter of compliance or financial risk. While fines can indeed reach significant levels up to €10 million or 2% of global turnover, that is not the greatest danger. The real risk lies in the loss of trust. A serious incident can disrupt essential services, expose sensitive data, and destroy reputations built over many years in a matter of hours.

In this sense, Decree-Law 125/2025 should not be seen as a bureaucratic burden, but as a strategic guide. It acts as a compass, compelling organisations to think systematically about risk, resilience, and responsibility clearly involving those who make decisions.

In the end, the choice is clear and unavoidable: continue reacting, patching vulnerabilities as they arise, or invest in a solid structure, designed from the outset to withstand present and future challenges. Resilience is no longer a finishing touch. It is, definitively, the structure itself.

Leonor Carvalho
Sénior Information Security Consultant
Devoteam Cyber Trust