

NIS2 | SCOPE | GOVERNANCE | ACCOUNTABILITY

# NIS2 in Portugal: 5 mistakes that leave companies exposed

The biggest mistake is rarely technical. It starts with a weak scope and applicability assessment.

**Mistake 1**

## **Treating NIS2 as an IT-only issue**

If legal, compliance, risk and management are left out, the analysis starts on the wrong foot. The real question is not “do we have controls?” but “who decides, who responds and how do we prove it?”

**Mistake 2**

## **Assuming NIS2 only affects critical infrastructure**

Many organisations exclude themselves too early from the regulatory perimeter. Services, dependencies, operational continuity, third parties and business impact matter more than labels.

**Mistake 3**

## **Assessing scope without mapping services and dependencies**

Without a functional inventory, the scope decision is hard to defend. Map critical processes, core systems, operational flows, single points of failure, suppliers, cloud and managed services.

**Mistake 4**

## **Not connecting NIS2 to governance and accountability**

When responsibility is diffuse, the response will be diffuse too. Regulatory maturity is decision maturity: criteria, responsibilities, escalation and evidence.

**Mistake 5**

## **Not documenting the analysis and adequacy plan**

Without a decision trail, the organisation loses defence and execution capacity. Record criteria, assumptions, services assessed, exclusions, dependencies, conclusions, owners and roadmap.

## Conclusion

# The test that matters is not technical

The real test is whether the organisation understands if it is in scope, what it must do and how it can demonstrate it. Ahkoris helps turn regulatory scope into defensible analysis, clear priorities and executable governance.