FREE GUIDE · NIS2 · DECREE-LAW 125/2025

# 20 OT questions for NIS2

A self-assessment for plants in scope of Portuguese Decree-Law 125/2025: governance, inventory, segmentation, remote access, monitoring, notification, recovery and supply chain.

For the cybersecurity officer, the plant director and the IT/OT lead.

## What Decree-Law 125/2025 means for a plant with OT

Decree-Law 125/2025 of 4 December transposes the NIS2 Directive and sets out Portugal's new Cybersecurity Legal Regime.[1,4] It has been in force since April 2026. CNCS Regulation 756/2026, published on 22 June 2026, sets out how it applies: the registration platform, incident notification and minimum cybersecurity measures.[2]

Registration of in-scope entities, appointing a cybersecurity officer, a permanent point of contact and incident notification already apply. The risk-management measures, including supply-chain security, take effect on 22 June 2028.[1]

The law does not mention PLCs, SCADA or VLANs. But management will have to show that it knows the industrial network, has separated it from the corporate network, controls who accesses it and can detect and report an incident in time. The 20 questions below help you see where you stand today and what is still missing before 2028.

**KEY DATES**

| | |
|---|---|
| 4 Dec 2025 | Decree-Law 125/2025 published |
| Apr 2026 | Entry into force (120 days after publication) |
| 22 Jun 2026 | CNCS Regulation 756/2026 published |
| 22 Jun 2028 | Risk-management measures take effect |

**HOW TO USE IT**

Answer each question with Yes, Partly or No. Every Partly or No is an input for your action plan. Your entity's formal classification (essential, important or out of scope) should be confirmed with legal support and on the CNCS platform.

## Self-assessment summary

Once you have answered, count the answers in each group. The groups with the most No answers show where to start.

| | | YES | PARTLY | NO |
|---|---|---|---|---|
| 01–04 | Governance and responsibility | | | |
| 05–08 | Asset and flow inventory | | | |
| 09–12 | Segmentation and remote access | | | |
| 13–16 | Monitoring, logging and notification | | | |
| 17–20 | Recovery and supply chain | | | |

## 01 Governance and responsibility

### 01 Has your entity confirmed whether it is essential, important or out of scope, and registered on the CNCS platform?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Registration and self-identification already apply, and they determine the compliance level (basic, substantial or high) and the minimum measures that apply to you. [2]

WHAT GOOD LOOKS LIKE Registration completed, classification received and filed, with a clear list of the industrial sites included.

### 02 Has a cybersecurity officer been appointed, and is the OT network within their remit?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS The law requires an officer who reports directly to management. [1] If OT is off their radar, it is off the plan.

WHAT GOOD LOOKS LIKE Officer appointed and notified to CNCS within 20 working days, with a named OT technical contact at each plant.

### 03 Has management approved the risk-management measures, and has it received cybersecurity training?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Management bodies approve the measures, oversee their implementation and must be trained. [1,4]

WHAT GOOD LOOKS LIKE Approval recorded in the minutes, a plan with owners and dates, and documented management training.

### 04 Is there a permanent point of contact that also covers the plant's shifts?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS The authority can activate the point of contact 24 hours a day, 7 days a week. [1] An OT incident does not keep office hours.

WHAT GOOD LOOKS LIKE Team and alternative contacts notified to CNCS, with a rota that includes someone who can decide to stop or isolate a line.

## 02 Asset and flow inventory

### 05 Is there an up-to-date inventory of OT assets: PLCs, HMIs, SCADA, servers, switches and gateways?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS You cannot protect or recover what you do not know exists. The inventory underpins every other measure. [5]

WHAT GOOD LOOKS LIKE A per-site inventory with vendor, model, firmware, location and owner, reviewed after every significant change and at least once a year.

### 06 Are communication flows between OT, the corporate network, the cloud and the outside world mapped?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Undocumented flows are, in practice, the paths an attacker uses to reach production.

WHAT GOOD LOOKS LIKE A flow matrix with source, destination, protocol and justification, validated with traffic capture and not just interviews.

### 07 Do you know which OT systems run unsupported software or have known vulnerabilities?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Old operating systems and outdated firmware are common on lines that are 10 or 20 years old, and they cannot always be patched.

WHAT GOOD LOOKS LIKE A list of unsupported assets, each with a compensating control (isolation, application allow-listing, restricted access) and a replacement plan.

### 08 Are assets classified by criticality for production and for people's safety?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Criticality sets priorities for segmentation, monitoring and recovery, and feeds the risk analysis.

WHAT GOOD LOOKS LIKE Each asset or cell has a simple rating (high, medium, low) agreed between production, maintenance and IT.

## 03 Segmentation and remote access

### 09 Is the OT network separated from the corporate network, with an industrial DMZ between them?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS On a flat network, ransomware that enters through the office can reach the production lines.

WHAT GOOD LOOKS LIKE No direct flows between IT and OT: everything passes through an industrial DMZ (level 3.5 in the Purdue model), with documented and reviewed firewall rules.

### 10 Is the industrial network divided into zones and conduits, in line with IEC 62443?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Separating OT from IT is not enough. Inside the plant, one compromised line should not contaminate the others. [6]

WHAT GOOD LOOKS LIKE Zones defined by function and criticality (lines, utilities, safety systems), conduits carrying only the traffic needed and a target security level per zone.

### 11 Is vendor and integrator remote access based on individual identity, approval and logging?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Forgotten modems, remote-control software installed on HMIs and shared VPN accounts are among the most common ways into OT.

WHAT GOOD LOOKS LIKE A single remote-access point, named accounts with multi-factor authentication, access enabled only when approved and sessions logged.

### 12 Are OT access rights reviewed and removed when no longer needed?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Generic accounts and access for technicians who have left build up over the years.

WHAT GOOD LOOKS LIKE Access management with periodic reviews, no default passwords and shared accounts kept to a justified minimum.

## 04 Monitoring, logging and notification

### 13 Can you detect anomalous activity on the OT network, such as a new device or a change to a PLC?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS Without visibility, many incidents are only discovered when production stops, and by then notification is already late.

WHAT GOOD LOOKS LIKE Passive monitoring of the industrial network, with alerts for new assets, new communications and program changes, routed to the people who handle them.

### 14 Are logs from OT systems, firewalls and remote access collected and protected?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS Without logs there is no investigation and no credible final report for the authority.

WHAT GOOD LOOKS LIKE Centralised logs with synchronised time, a defined retention period and restricted access, covering firewalls, remote access and SCADA servers.

### 15 Is there a procedure to classify an incident as significant and report it within the legal deadlines?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS The regime requires an initial notification within 24 hours of establishing a significant incident, an update within 72 hours where necessary, an end-of-significant-impact notification within 24 hours of the impact ending and a final report within 30 working days. [1]

WHAT GOOD LOOKS LIKE Written significance criteria, prepared notification templates, named people to submit on the CNCS platform and a timestamped record of each step.

### 16 Does the incident response plan include OT scenarios, and has it been tested with production?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS In OT, isolating a system can stop a line or affect people's safety. That decision cannot be improvised.

WHAT GOOD LOOKS LIKE A plan with criteria for isolating or keeping systems running, contacts for critical vendors and at least one annual exercise with IT, OT and production.

## 05 Recovery and supply chain

### 17 Are there backups of PLC programs, HMI and SCADA configurations and network devices?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS After an incident or a failure, recovering without the right program can mean days of downtime.

WHAT GOOD LOOKS LIKE Versioned backups updated after every change, stored outside the OT network, with at least one offline or immutable copy.

### 18 Has recovery been tested, and are restoration times known?

☐ Yes ☐ Partly ☐ No

WHY IT MATTERS A backup that has never been restored is an assumption, not a guarantee.

WHAT GOOD LOOKS LIKE Periodic restore tests on critical assets, with restoration time measured and compared with what production can accept.

### 19 Do contracts with OT suppliers include cybersecurity requirements?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Supply-chain security is one of the mandatory measures, and integrators and machine builders often have privileged access. [1,4]

WHAT GOOD LOOKS LIKE A list of critical suppliers and clauses on remote access, incident notification, updates and end of support, with periodic review.

### 20 When buying new machines and systems, is cybersecurity part of the specification?

☐ Yes
☐ Partly
☐ No

WHY IT MATTERS Every new machine brings software, remote access and dependencies that stay in the plant for years.

WHAT GOOD LOOKS LIKE Minimum purchasing requirements (for example, referencing IEC 62443-4-2), network documentation delivered and remote access validated before acceptance.

## + Next actions

Record here the actions that follow from your Partly and No answers, with an owner and a deadline.

| NO. | ACTION | OWNER | DEADLINE |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 06 Where to start

If you answered Partly or No to several questions, that is normal. Most plants start in the same place: knowing what is on the network, closing down remote access and gaining visibility. There is time before 22 June 2028 for a phased plan, but not for putting off the first step.

> **NIS2 technical measures for industrial networks, with fixed scope and fixed price.**

**OT network assessment**
Inventory, flows, risks and a prioritised plan. Answers questions 5 to 8 and prepares the rest.
musas.pt/en/ot-network-assessment/

**Segmentation and remote access**
Zones and conduits, industrial DMZ and controlled vendor access. Questions 9 to 12.
musas.pt/en/ot-segmentation-remote-access/

**OT monitoring**
Anomaly detection and logging that support incident notification. Questions 13 to 16.
musas.pt/en/ot-monitoring/

**NIS2 for industry**
What Decree-Law 125/2025 means for the OT network, in technical terms.
musas.pt/en/nis2/

**Initial technical consultation**
30 min · €60 + VAT. Tell us the context (number of sites, environments, what you want clarified) and leave with a first technical reading and a clear next step. Book at musas.pt.

We do not give legal advice or determine your entity's classification. We handle the technical side of the IT/OT network, working alongside your legal advisers, cybersecurity officer and integrator.

### Sources


1. Decree-Law 125/2025 of 4 December (Cybersecurity Legal Regime), Diário da República (PT): art. 11 (entry into force), art. 10(2) (when measures take effect) and, in the annexed regime, arts. 25, 27, 28, 31, 32 and 41 to 44.
   https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401
2. CNCS Regulation 756/2026 of 22 June, Diário da República, Series II (PT).
   https://diariodarepublica.pt/dr/detalhe/regulamento/756-2026-1134399056
3. National Cybersecurity Centre, CNCS (PT).
   https://www.cncs.gov.pt/
4. Directive (EU) 2022/2555 (NIS2), EUR-Lex: art. 20 (governance), art. 21 (measures) and art. 23 (reporting).
   https://eur-lex.europa.eu/eli/dir/2022/2555/oj
5. ENISA, NIS2 Technical Implementation Guidance.
   https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
6. ISA, ISA/IEC 62443 series of standards.
   https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards


General information, not legal advice. Deadlines and references checked in November 2026; always confirm the text in force in the Diário da República.