GUIA GRATUITO · NIS2 · DL 125/2025

20 perguntas OT para a NIS2

Autoavaliação para fábricas abrangidas pelo Decreto-Lei n.º 125/2025: governação, inventário, segmentação, acesso remoto, monitorização, notificação, recuperação e cadeia de abastecimento.

Para o responsável de cibersegurança, a direção fabril e o responsável de IT/OT.

O que o DL 125/2025 significa para uma fábrica com OT

O Decreto-Lei n.º 125/2025, de 4 de dezembro, transpõe a Diretiva NIS2 e aprova o novo Regime Jurídico da Cibersegurança. [1,4] Está em vigor desde abril de 2026. O Regulamento n.º 756/2026 do CNCS, publicado a 22 de junho de 2026, concretiza a sua aplicação: plataforma de registo, notificação de incidentes e medidas mínimas de cibersegurança. [2]

O registo das entidades abrangidas, a designação do responsável de cibersegurança, o ponto de contacto permanente e a notificação de incidentes já são exigíveis. As medidas de gestão de risco, incluindo a segurança da cadeia de abastecimento, produzem efeitos a 22 de junho de 2028. [1]

A lei não fala em PLC, SCADA ou VLAN. Mas a gestão terá de mostrar que conhece a rede industrial, que a separou da rede corporativa, que controla quem lhe acede e que consegue detetar e notificar um incidente a tempo. As 20 perguntas seguintes ajudam a perceber onde está hoje e o que falta até 2028.

DATAS-CHAVE

4 dez 2025	Publicação do DL 125/2025
abr 2026	Entrada em vigor (120 dias após a publicação)
22 jun 2026	Publicação do Regulamento n.º 756/2026 do CNCS
22 jun 2028	Medidas de gestão de risco produzem efeitos

COMO USAR

Responda a cada pergunta com Sim, Parcial ou Não. Cada «Parcial» ou «Não» é uma entrada para o plano de ações. A qualificação formal da entidade (essencial, importante ou fora do âmbito) deve ser confirmada com apoio jurídico e na plataforma do CNCS.

Resumo da autoavaliação

Depois de responder, conte as respostas por grupo. Os grupos com mais «Não» indicam onde começar.

		SIM	PARCIAL	NÃO
01–04	Governação e responsabilidade			
05–08	Inventário de ativos e fluxos			
09–12	Segmentação e acesso remoto			
13–16	Monitorização, registos e notificação			
17–20	Recuperação e cadeia de abastecimento			

01 Governação e responsabilidade

01 A entidade já confirmou se é essencial, importante ou não abrangida, e fez o registo na plataforma do CNCS?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ O registo e a autoidentificação já são exigíveis e determinam o nível de conformidade (básico, substancial ou elevado) e as medidas mínimas aplicáveis. [2]

O QUE É BOM Registo feito, qualificação recebida e arquivada, com indicação clara dos sites industriais incluídos.

02 Está designado o responsável de cibersegurança, e a rede OT faz parte do seu âmbito?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ A lei exige um responsável que reporte diretamente à gestão. [1] Se a OT ficar fora do seu radar, fica fora do plano.

O QUE É BOM Responsável designado e comunicado ao CNCS no prazo de 20 dias úteis, com um interlocutor técnico de OT identificado em cada fábrica.

03 A gestão aprovou as medidas de gestão de risco e tem formação em cibersegurança?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Os órgãos de gestão aprovam as medidas, acompanham a sua aplicação e devem ter formação. [1,4]

O QUE É BOM Aprovação registada em ata, plano com responsáveis e datas, e formação da gestão documentada.

04 Existe um ponto de contacto permanente que cubra também os turnos da fábrica?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ A autoridade pode ativar o ponto de contacto 24 horas por dia, 7 dias por semana. [1] Um incidente na OT não escolhe o horário de expediente.

O QUE É BOM Equipa e contactos alternativos comunicados ao CNCS, com uma escala que inclui quem pode decidir parar ou isolar uma linha.

02 Inventário de ativos e fluxos

05 Existe um inventário atualizado dos ativos OT: PLC, HMI, SCADA, servidores, switches e gateways?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Não se protege nem se recupera o que não se sabe que existe. O inventário é a base de todas as outras medidas. [5]

O QUE É BOM Inventário por site com fabricante, modelo, firmware, localização e responsável, revisto após cada alteração relevante e pelo menos uma vez por ano.

06 Estão mapeados os fluxos de comunicação entre a OT, a rede corporativa, a cloud e o exterior?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Os fluxos não documentados são, na prática, os caminhos que um atacante usa para chegar à produção.

O QUE É BOM Matriz de fluxos com origem, destino, protocolo e justificação, validada com captura de tráfego e não apenas com entrevistas.

07 Sabe que sistemas OT correm software sem suporte ou com vulnerabilidades conhecidas?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Sistemas operativos antigos e firmware desatualizado são comuns em linhas com 10 ou 20 anos e nem sempre podem ser atualizados.

O QUE É BOM Lista de ativos sem suporte, com medida compensatória para cada um (isolamento, lista de aplicações permitidas, acesso restrito) e plano de substituição.

08 Os ativos estão classificados por criticidade para a produção e para a segurança de pessoas?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ A criticidade define prioridades de segmentação, monitorização e recuperação, e alimenta a análise de risco.

O QUE É BOM Cada ativo ou célula com uma classificação simples (alta, média, baixa) acordada entre produção, manutenção e IT.

03 Segmentação e acesso remoto

09 A rede OT está separada da rede corporativa, com uma DMZ industrial entre ambas?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Numa rede plana, um ransomware que entra pelo escritório pode chegar às linhas de produção.

O QUE É BOM Nenhum fluxo direto entre IT e OT: tudo passa por uma DMZ industrial (o nível 3.5 do modelo Purdue), com regras de firewall documentadas e revistas.

10 A rede industrial está dividida em zonas e condutas, segundo a IEC 62443?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Separar a OT da IT não chega. Dentro da fábrica, uma linha comprometida não deve contaminar as outras. [6]

O QUE É BOM Zonas definidas por função e criticidade (linhas, utilidades, sistemas de segurança), condutas com o tráfego mínimo necessário e um nível de segurança alvo por zona.

11 O acesso remoto de fornecedores e integradores é feito com identidade individual, aprovação e registo?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Modems esquecidos, software de controlo remoto instalado na HMI e VPN partilhadas estão entre as vias de entrada mais comuns na OT.

O QUE É BOM Um ponto único de acesso remoto, contas nominativas com autenticação multifator, acesso ativado só quando aprovado e sessões registadas.

12 Os acessos à OT são revistos e removidos quando deixam de ser necessários?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Contas genéricas e acessos de técnicos que já saíram acumulam-se ao longo dos anos.

O QUE É BOM Gestão de acessos com revisão periódica, sem palavras-passe por omissão e com contas partilhadas reduzidas ao mínimo justificado.

04 Monitorização, registos e notificação

13 Consegue detetar atividade anómala na rede OT, como um novo dispositivo ou uma alteração a um PLC?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Sem visibilidade, muitos incidentes só são descobertos quando a produção para, e aí a notificação já começa atrasada.

O QUE É BOM Monitorização passiva da rede industrial, com alertas para novos ativos, novas comunicações e alterações de programa, encaminhados para quem os trata.

14 Os registos (logs) dos sistemas OT, das firewalls e do acesso remoto são recolhidos e protegidos?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Sem registos não há investigação nem um relatório final credível para a autoridade.

O QUE É BOM Registos centralizados, com hora sincronizada, retenção definida e acesso restrito, incluindo firewalls, acesso remoto e servidores SCADA.

15 Existe um procedimento para classificar um incidente como significativo e notificá-lo dentro dos prazos legais?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ O regime exige notificação inicial até 24 horas após a verificação do incidente significativo, atualização até 72 horas quando necessário, notificação do fim do impacto significativo até 24 horas após o seu termo e relatório final em 30 dias úteis. [1]

O QUE É BOM Critérios de significância escritos, modelos de notificação preparados, responsáveis pela submissão na plataforma do CNCS e registo da hora de cada passo.

16 O plano de resposta a incidentes inclui cenários OT e foi testado com a produção?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Na OT, isolar um sistema pode parar uma linha ou afetar a segurança de pessoas. A decisão não pode ser improvisada.

O QUE É BOM Plano com critérios para isolar ou manter em funcionamento, contactos dos fornecedores críticos e pelo menos um exercício anual com IT, OT e produção.

05 Recuperação e cadeia de abastecimento

17 Existem cópias de segurança dos programas de PLC, das configurações de HMI e SCADA e dos equipamentos de rede?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Depois de um incidente ou de uma avaria, recuperar sem o programa certo pode significar dias de paragem.

O QUE É BOM Cópias versionadas e atualizadas após cada alteração, guardadas fora da rede OT, com pelo menos uma cópia offline ou imutável.

18 A recuperação foi testada e os tempos de reposição são conhecidos?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Uma cópia que nunca foi restaurada é uma suposição, não uma garantia.

O QUE É BOM Testes de restauro periódicos nos ativos críticos, com o tempo de reposição medido e comparado com o que a produção aceita.

19 Os contratos com fornecedores de OT incluem requisitos de cibersegurança?

☐ Sim
☐ Parcial
☐ Não

PORQUÊ A segurança da cadeia de abastecimento é uma das medidas obrigatórias, e integradores e fabricantes de máquinas têm muitas vezes acesso privilegiado. [1,4]

O QUE É BOM Lista de fornecedores críticos e cláusulas sobre acesso remoto, notificação de incidentes, atualizações e fim de suporte, com avaliação periódica.

20 **Na compra de máquinas e sistemas novos, a cibersegurança faz parte do caderno de encargos?**

☐ Sim
☐ Parcial
☐ Não

PORQUÊ Cada máquina nova traz software, acessos remotos e dependências que ficam na fábrica durante anos.

O QUE É BOM Requisitos mínimos na compra (por exemplo, com referência à IEC 62443-4-2), documentação de rede entregue e acesso remoto validado antes da receção.

+ Próximas ações

Registe aqui as ações que resultam das respostas «Parcial» e «Não», com um responsável e um prazo.

N.º	AÇÃO	RESPONSÁVEL	PRAZO

06 Por onde começar

Se respondeu «Parcial» ou «Não» a várias perguntas, é o habitual. A maioria das fábricas começa pelo mesmo sítio: saber o que tem na rede, fechar o acesso remoto e ganhar visibilidade. Até 22 de junho de 2028 há tempo para um plano faseado, mas não para adiar o primeiro passo.

> **Medidas técnicas NIS2 para redes industriais, com âmbito e preço fechados.**

Avaliação de rede OT
Inventário, fluxos, riscos e plano priorizado. Responde às perguntas 5 a 8 e prepara as restantes.
musas.pt/avaliacao-rede-ot/

Segmentação e acesso remoto
Zonas e condutas, DMZ industrial e acesso de fornecedores controlado. Perguntas 9 a 12.
musas.pt/segmentacao-acesso-remoto/

Monitorização OT
Deteção de anomalias e registos que suportam a notificação de incidentes. Perguntas 13 a 16.
musas.pt/monitorizacao-ot/

NIS2 na indústria
O que o DL 125/2025 significa para a rede OT, em linguagem técnica.
musas.pt/nis2/

Consulta técnica inicial
30 min · 60 € + IVA. Conte o contexto (número de sites, ambientes, o que quer ver esclarecido) e saia com uma primeira leitura técnica e um próximo passo claro. Marcação em musas.pt.

Não prestamos aconselhamento jurídico nem determinamos a qualificação da entidade. Trabalhamos a parte técnica da rede IT/OT, em articulação com o jurídico, o responsável de cibersegurança e o integrador.

Fontes

1. Decreto-Lei n.º 125/2025, de 4 de dezembro (Regime Jurídico da Cibersegurança), Diário da República: art. 11.º (entrada em vigor), art. 10.º, n.º 2 (produção de efeitos) e, no regime anexo, arts. 25.º, 27.º, 28.º, 31.º, 32.º e 41.º a 44.º.
   https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401
2. Regulamento n.º 756/2026, de 22 de junho, do CNCS, Diário da República, 2.ª série.
   https://diariodarepublica.pt/dr/detalhe/regulamento/756-2026-1134399056
3. Centro Nacional de Cibersegurança (CNCS).
   https://www.cncs.gov.pt/
4. Diretiva (UE) 2022/2555 (NIS2), EUR-Lex: art. 20.º (governação), art. 21.º (medidas) e art. 23.º (notificação).
   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, série de normas ISA/IEC 62443.
   https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Informação geral, não constitui aconselhamento jurídico. Prazos e referências verificados em novembro de 2026; confirme sempre o texto em vigor no Diário da República.