DIANA BY CYBERS3C

CHECKLIST · CONFORMIDADE

Checklist NIS2 para CISOs.

Um guia prático para avaliar a prontidão da sua organização face às obrigações da diretiva NIS2 em gestão de risco e testes de segurança — em linguagem de negócio, com o que os auditores esperam ver como prova.

EDIÇÃO
Julho 2026

ÂMBITO
Diretiva (UE) 2022/2555 — NIS2

AUDIÊNCIA
CISOs & administração

A NIS2 EM UMA PÁGINA

O que mudou — e porque lhe diz respeito.

A **Diretiva (UE) 2022/2555 (NIS2)** é aplicável na União Europeia desde **17 de outubro de 2024** e alarga substancialmente o universo de entidades abrangidas — de operadores de serviços essenciais a médias e grandes empresas de setores como energia, transportes, banca, saúde, infraestruturas digitais, administração pública, alimentar, químico e espacial.

Três mudanças importam especialmente a quem gere segurança:

1 · Responsabilidade direta da gestão de topo

Os órgãos de administração devem *aprovar* e *supervisionar* as medidas de gestão de risco — e podem ser responsabilizados pelo incumprimento (art. 20.º). «A segurança é do departamento de TI» deixou de ser defensável.

2 · Gestão de risco contínua, não pontual

O art. 21.º exige medidas técnicas e organizativas «adequadas e proporcionadas» — incluindo políticas de análise de risco, tratamento de incidentes, continuidade, segurança na cadeia de fornecimento e **políticas e procedimentos para avaliar a eficácia das medidas**. Avaliar eficácia uma vez por ano dificilmente convence um supervisor.

3 · Prova documentada de diligência

Perante um incidente ou uma auditoria, a questão não é «o que dizia a política?», é «**o que foi efetivamente testado, quando, por quem e com que resultado?**». Sem evidência, a diligência não se demonstra.

NOTA

Este documento é informativo e não constitui aconselhamento jurídico. A transposição nacional pode introduzir requisitos adicionais — confirme o enquadramento aplicável à sua entidade com o seu apoio legal.

Governação & gestão de risco

A · Governação e responsabilidade

- [ ] **A administração aprova formalmente as medidas de gestão de risco de cibersegurança**
  Ata ou registo de aprovação — é o primeiro documento que um auditor pede.

- [ ] **A gestão de topo recebe relatórios de risco que compreende**
  Relatórios com impacto de negócio e prioridades, não listas técnicas de CVEs.

- [ ] **Existe formação em cibersegurança para os órgãos de gestão**
  A NIS2 exige-a expressamente aos membros dos órgãos de direção (art. 20.º, n.º 2).

B · Gestão de risco contínua

- [ ] **A análise de risco é um processo vivo, não um exercício anual**
  O risco muda a cada deploy, a cada novo serviço exposto, a cada CVE relevante.

- [ ] **O inventário de ativos expostos está atualizado (superfície de ataque)**
  Não se protege o que não se conhece; a descoberta contínua alimenta tudo o resto.

- [ ] **A cadeia de fornecimento entra na avaliação de risco**
  O art. 21.º inclui explicitamente a segurança da cadeia de fornecimento.

C · Frequência e profundidade dos testes

- [ ] **Testa a segurança mais do que uma vez por ano**
  Entre dois pentests anuais há ~350 dias de exposição não validada.

- [ ] **Os testes cobrem o perímetro externo e a rede interna**
  A maioria dos incidentes graves envolve movimento lateral pós-perímetro.

- [ ] **Novos ativos críticos são testados quando entram em produção — não no ciclo seguinte**
  O intervalo entre exposição e validação é a janela do atacante.

Validação, resposta & prova

D · Validação por exploração

- [ ] **Confirma que as vulnerabilidades são realmente exploráveis, com evidência**
  Um scanner lista possibilidades; a exploração controlada prova o risco real e elimina falsos positivos.
- [ ] **A priorização usa explorabilidade real, não apenas CVSS**
  Corrigir primeiro o que está provado como explorável no seu ambiente.
- [ ] **As correções são revalidadas após a remediação**
  «Corrigido» sem reteste é uma hipótese, não um facto.

E · Deteção e resposta

- [ ] **Os achados de teste alimentam o SOC / Blue Team**
  Exposição validada é contexto valioso para deteção e para exercícios de resposta.
- [ ] **Os prazos de notificação de incidentes estão operacionalizados**
  Alerta precoce em 24h e notificação em 72h (art. 23.º) não se improvisam durante o incidente.

F · Trilho de auditoria e diligência

- [ ] **Cada ação de teste fica registada: o quê, quando, por quem, com que autorização**
  É a diferença entre afirmar diligência e demonstrá-la.
- [ ] **Consegue apresentar a um auditor, hoje, a evidência dos últimos testes**
  Relatórios com âmbito, método, achados, evidência e estado de correção.
- [ ] **As exceções e aceitações de risco estão documentadas e assinadas**
  Aceitar um risco é legítimo; não o documentar, não.

> **O QUE OS AUDITORES ESPERAM VER**
>
> Âmbito autorizado por escrito · calendário e frequência dos testes · método (descoberta e validação) · evidência de exploração controlada · priorização justificada · prova de remediação e reteste · relatório executivo apresentado à administração.

ONDE OS TESTES CONTÍNUOS ENCAIXAM

Da obrigação à evidência.

A NIS2 não exige uma ferramenta específica — exige **eficácia demonstrável**. Os testes de intrusão contínuos respondem diretamente a quatro obrigações:

A NIS2 EXIGE	OS TESTES CONTÍNUOS ENTREGAM
Gestão de risco contínua	Avaliação recorrente da exposição real, não fotografias anuais.
Avaliar a eficácia das medidas	Exploração controlada que prova se as defesas resistem.
Responsabilidade da administração	Relatórios executivos com risco validado e priorizado.
Prova de diligência	Trilho de auditoria completo de cada ação executada.

PRÓXIMO PASSO

Quer saber onde está a sua organização?

Faça a avaliação NIS2 gratuita em **diana.red/avaliacao-nis2** (2 minutos) ou agende uma demonstração da DIANA — pentest autónomo com IA, supervisionado por humanos, com dados em Portugal e na UE.

diana.red/contactos · hello@cybersec.pt · +351 21 594 4726