Checklist de Implementação NIS2 - Portugal (2026)

Um roteiro prático para avaliar aplicabilidade, planear medidas de gestão de risco e preparar evidências e reporte de incidentes.

Organização: _____	Setor: _____	Classificação: [ ] Essencial [ ] Importante [ ] Por confirmar
Responsável cibersegurança: _____	Ponto de contacto 24/7: _____	Data de revisão: ___/___/_____

1) Enquadramento e aplicabilidade

- ☐ Confirmar se a organização opera em setor crítico (Anexo I/II) e se cumpre critérios de dimensão (PME/Média/Grande) ou tipologia digital relevante.
- ☐ Mapear serviços críticos (processos e sistemas) e dependências (cloud, telecom, fornecedores TIC, MSP/MSSP).
- ☐ Definir classificação provisória: Entidade Essencial / Importante / Fora do âmbito (com justificação).
- ☐ Identificar autoridade competente e requisitos de autoidentificação / registo (quando aplicável).

2) Governance, responsabilidades e políticas

- ☐ Aprovação formal pela gestão de: política de cibersegurança, apetite ao risco e prioridades de investimento.
- ☐ Nomear Responsável de Cibersegurança e definir mandato, reporte e recursos.
- ☐ Designar Ponto de Contacto 24/7 e definir escalões (on-call).
- ☐ Criar comité de cibersegurança (TI, Segurança, Operações, Compliance/Jurídico) com reunião mensal e atas.

3) Gestão de risco e planeamento

- ☐ Adotar metodologia de avaliação de risco (critérios, probabilidade/impacto, aceitação).
- ☐ Manter inventário de ativos (hardware, software, dados) e classificação de criticidade.
- ☐ Criar plano de tratamento de risco com responsáveis, prazos e evidências (quick wins + roadmap 6-12 meses).
- ☐ Integrar risco de terceiros: critérios de avaliação, cláusulas contratuais, SLAs e auditorias.

4) Controlos técnicos e operacionais (baseline)

- ☐ MFA e controlo de acessos (least privilege), revisão periódica de permissões e contas privilegiadas.

- ☐ Gestão de vulnerabilidades: patching, hardening, scans regulares e remediação monitorizada.
- ☐ Backups: estratégia 3-2-1, testes de restauração e proteção contra ransomware (immutability/air-gap quando possível).
- ☐ Monitorização e logging: centralização, retenção adequada, alertas e procedimentos de resposta.
- ☐ Segurança de rede: segmentação, firewalling, proteção endpoint e configurações seguras.
- ☐ Segurança no desenvolvimento/alterações: controlo de mudanças, SDLC seguro e revisões.

5) Incidentes e obrigações de notificação

- ☐ Definir critério de 'incidente significativo' (impacto, duração, extensão, clientes afetados).
- ☐ Estabelecer processo de notificação: triagem, aprovação, envio e registo de comunicações.
- ☐ Criar playbooks (ransomware, indisponibilidade, fuga de dados, fraude) e treinar equipas (tabletop 2x/ano).
- ☐ Manter evidências: linha temporal, decisores, logs, medidas de mitigação e comunicação externa.

6) Continuidade, resiliência e cadeia de abastecimento

- ☐ Definir RTO/RPO por serviço crítico e testar planos de continuidade/DR pelo menos anualmente.
- ☐ Garantir redundância onde necessário (single points of failure) e manter planos para falhas de fornecedores críticos.
- ☐ Avaliar fornecedores críticos: questionários, provas (certificações, relatórios), planos de incidentes e subcontratação.
- ☐ Planear requisitos de segurança em compras (procurement) e critérios de seleção.

7) Pessoas, formação e cultura

- ☐ Plano anual de formação por função (gestão, TI, operações, utilizadores) e registos de participação.
- ☐ Simulações de phishing e campanhas de higiene cibernética (com métricas).
- ☐ Políticas de onboarding/offboarding, teletrabalho e utilização aceitável.

8) Evidências e auditoria interna

- ☐ Repositório de evidências: políticas, atas, inventários, avaliação de risco, planos, logs de treino e resultados de testes.

- ☐ KPIs: MTTD/MTTR, tempo de aplicação de patches, cobertura MFA, sucesso de backups, maturidade de fornecedores.
- ☐ Auditoria interna (ou revisão independente) anual para validar maturidade e gaps.

9) Plano rápido 30-60-90 dias

Horizonte	Objetivo	Entregáveis (evidência)
0-30 dias	Triage NIS2 + governance mínima	Scope/applicabilidade; nomeações; inventário inicial; política e comité; plano de incidentes (v0)
31-60 dias	Risco + controlos prioritários	Avaliação de risco; plano de tratamento; MFA/privileged; backups testados; logging básico; gestão de vulnerabilidades
61-90 dias	Operacionalizar e testar	Tabletop; testes DR; avaliação fornecedores críticos; formação; dashboard KPI; pacote de evidências v1

Pacote de evidências mínimas (sugestão)

- ☐ Mapa de serviços críticos + dependências (inclui cloud e fornecedores TIC).
- ☐ Metodologia e relatório de avaliação de risco + plano de tratamento.
- ☐ Políticas-chave: cibersegurança, controlo de acessos, backups, logging/monitorização, gestão de vulnerabilidades, continuidade.
- ☐ Plano de resposta a incidentes + registos de exercícios (tabletop) + pós-incidente (lessons learned).
- ☐ Relatórios de testes de restauração e exercícios de continuidade/DR.
- ☐ Registos de formação e campanhas de sensibilização + métricas.
- ☐ Avaliação e monitorização de fornecedores críticos (questionários, cláusulas, evidências).

Notas finais

Esta checklist foi desenhada como instrumento de trabalho. Adapte-a ao seu contexto e mantenha um plano de melhoria contínua. Fontes de referência: Diretiva (UE) 2022/2555 (NIS2), transposição nacional (Portugal) e orientação técnica da ENISA sobre medidas de gestão de risco.