

CHECKLIST + EVIDÊNCIA

DORA Implementation Pack

Guia prático + checklist para implementação do DORA em Portugal

Próximo passo

Use esta checklist para acelerar a conformidade e preparar evidência para supervisão.

[Agendar Diagnóstico DORA](#)

[Falar com a iCompliance](#)

Checklist rápida

1. Defina o perímetro: entidades, serviços e Funções Críticas ou Importantes (CIFs).
2. Faça um gap assessment por pilar (governança, incidentes, testes, terceiros, threat intel).
3. Priorize um roadmap 90/180 dias com quick wins e remediações estruturais.
4. Organize evidência: políticas, registos, relatórios e decisões do órgão de gestão.

DORA em 5 pilares

Governança & Risco TIC

Framework, políticas, responsabilidades e controlos.

Incidentes & Reporte

Deteção, classificação, notificações e RCA.

Testes de Resiliência

Plano anual de testes e remediações.

Terceiros TIC

Contratos, registos, monitorização e exit plans.

Threat Intelligence

Partilha e monitorização de ameaças (quando aplicável).

Dica: comece pelo perímetro + incidentes + contratos críticos. São as áreas que mais falham em inspeção.

Perímetro e serviços críticos

- ☐ Mapear entidades e linhas de negócio abrangidas.
- ☐ Identificar serviços e CIFs (funções críticas ou importantes).
- ☐ Inventariar ativos TIC, dados, integrações e dependências.
- ☐ Definir RTO/RPO por serviço crítico e dependências associadas.

Governação e accountability

- ☐ Aprovar o programa DORA ao nível do órgão de gestão (atas e decisões).
- ☐ Definir modelo de governação (comités, reporting, escalonamento).
- ☐ Nomear responsáveis (owners) por risco TIC e por cada serviço crítico.
- ☐ Definir métricas/KRIs e reporting periódico para gestão.

Controlos essenciais de risco TIC

- ☐ Política de gestão de acessos (MFA, least privilege, revisões).
- ☐ Gestão de vulnerabilidades e patching (SLA por criticidade).
- ☐ Logging e monitorização (eventos, alertas, retenção).
- ☐ Gestão de alterações (change management e rollback).
- ☐ Backups e testes de restauro (frequência, evidência, RTO/RPO).
- ☐ Gestão de configurações e hardening (baselines).
- ☐ Continuidade e recuperação (BCP/DRP testados com o negócio).
- ☐ Segurança de dados (encriptação, chaves, classificação, DLP quando aplicável).

Incidentes TIC e reporte

- ☐ Definir taxonomia e critérios de severidade/classificação.
- ☐ Garantir capacidade de decisão e resposta 24/7 (on-call).
- ☐ Criar playbooks por cenário (ransomware, indisponibilidade, fuga de dados, falha fornecedor).
- ☐ Preparar templates de reporte (inicial, intermédio, final) e responsabilidades.
- ☐ Executar exercícios (tabletop) focados em tempos de classificação e reporte.
- ☐ Implementar RCA e plano de remediação com prazos e owners.

Testes de resiliência operacional digital

- ☐ Plano anual de testes (técnicos e processuais) aprovado e calendarizado.
- ☐ Testes de backup/restore, failover e continuidade (com evidência).
- ☐ Pentests/avaliações técnicas com fecho de remediações.
- ☐ Simulações de incidentes e testes a comunicação/escalonamento.

Gestão de risco de terceiros TIC

- ☐ Inventário de fornecedores TIC e avaliação de criticidade por serviço/CIF.
- ☐ Due diligence de segurança e resiliência (questionários, evidência, auditorias).
- ☐ Contratos com cláusulas essenciais (SLAs, notificação de incidentes, auditoria, subcontratação, localização, saída).
- ☐ Monitorização contínua de desempenho e risco (KPIs, alertas, revisões).
- ☐ Exit plan para serviços críticos (alternativas, migração, testes de saída).

Pacote de evidência (para supervisão/auditoria)

- Mapa de perímetro e CIFs + inventário de ativos/dependências.
- Políticas e procedimentos (risco TIC, acessos, mudanças, backups, continuidade, incidentes).
- Registos: incidentes, testes, vulnerabilidades, acessos, alterações, fornecedores.
- Relatórios de testes e remediações (com prazos, owners e evidência de fecho).
- Atas e decisões do órgão de gestão (aprovação e acompanhamento).

Se quiser, a iCompliance.eu pode executar um DORA Readiness & Gap Assessment e entregar o roadmap 90/180 dias.