NIS2 em Portugal:
5 erros que deixam empresas expostas

O maior erro raramente é técnico.
Começa numa análise fraca de enquadramento.

ÂMBITO | GOVERNANCE | ACCOUNTABILITY

ERRO 1

Tratar a NIS2 como m assunto só de IT

Se juridico, compliance, risco e gestão ficam fora, a análise nasce coxa.

O problema não começa no firewall.

Começa na governance: enquadramento legal, responsabilidade interna, cadeia de decisão e capacidade de capacidade de demonstrar o que foi avaliado.

IT sozinho não fecha o perimetro.

Pode conhecer sistemas, mas não decide sozinho o alcance regulatorio ou o nivel de exposição.

Sem sponsor executivo, há fricção.

Ficam controlos dispersos, prioridades concorrentes e baixa capacidade de execução.

O sinal de maturidade é simples.

A organização trata a NIS2 como um tema de governance operacional - não como checklist tecnica isolada.

A pergunta certa nao e "temos controlos?". E "quem decide, quem responde e como se prova?"

ERRO 2

Assumir que a NIS2 só afeta infraestruturas críticas

Muitas organizações excluem-se cedo demais do perimetro regulatório.

Erro de enquadramento

A organização olha para o nome do setor e ignora o papel real do servico, a criticidade operacional e o impacto potencial do incidente.

Erro de conforto

Parte-se do principio de que "isto é para os outros" e deixa-se de fazer a análise que realmente importa.

O perimetro precisa de leitura funcional.

Servicos, dependências, continuidade operacional, relações com terceiros e impacto no negocio valem mais do que intuições ou etiquetas simplistas.

Mau diagnostico = má preparação.

Se a empresa se autoexclui sem base robusta, perde tempo util e aumenta exposição quando o escrutinio chega.

ERRO 3

Avaliar o âmbito sem mapear serviços e dependências

Sem inventário funcional, a decisão sobre o âmbito e pouco defensável.

Mapeia o que sustenta o serviço

Processos criticos, sistemas nucleares, fluxos operacionais, pontos únicos de falha e interdependências internas.

Mapeia quem participa no serviço

Fornecedores, cloud, MSSP, outsourcers, integradores e qualquer terceiro que mexa na disponibilidade ou segurança.

Sem este trabalho, o debate fica superficial.

Discute-se a lei em abstrato, mas não se percebe como a operação real da empresa encaixa / ou não encaixa no enquadramento.

A qualidade do âmbito depende da qualidade do mapa.

É por isso que uma boa análise começa muito antes da matriz de compliance.

ERRO 4

Não ligar NIS2 a governance e accountability

Quando a responsabilidade e difusa, a resposta também o será.

Sem dono claro, há ilhas.

IT, juridico, compliance, risco e operação trabalham em paralelo e ninguém fecha a decisão nem o plano.

A gestão não pode entrar no fim

Se o tema sobe tarde, a organização decide sob pressão e com pouca visão do impacto real.

Accountability não é detalhe

Implica criterios, responsabilidades, escalonamento e prova de que a empresa avaliou com método.

Maturidade regulatoria = maturidade de decisão.

O regulador vê mais do que controlos tecnicos. Vê como a organização pensa, decide e demonstra o que fez.

ERRO 5

Não documentar a análise e o plano de adequação

Sem rasto de decisão, a organização perde defesa e capacidade de execução.

O que deve ficar registado

Criterios usados, pressupostos adotados, servicçs avaliados, exclusões, dependências e conclusão sobre o âmbito.

O que tambem importa guardar

Dono de cada ação, prioridades, roadmap, decisões pendentes e mecanismos de revisão da análise.

Documentar não é burocracia.

É o que transforma uma intuição numa posição defensável e uma reação dispersa num plano executavel.

Sem prova, a memória organizacional evapora.

E cada revisão volta a comecar do zero.

CONCLUSÃO

O teste que interessa não é técnico.

Mas sim:

Percebermos se estamos abrangidos, o que temos de fazer e como o demonstramos?

Na Ahkoris, ajudamos a transformar enquadramento regulatório numa análise defensável, prioridades claras e governance executavel.

Se a decisão nunca foi revista com rigor,
esse é o primeiro risco a corrigir.