NIS2 + CRA

A cibersegurança europeia já já não cabe em diplomas isolados.

NIS2, Cyber Resilience Act e reforma europeia estão a convergir num modelo de responsabilidade distribuída.

COMPLIANCE | GOVERNANCE | EXECUTIVE VIEW

Driven by ethics. Building compliance.

LEITURA EXECUTIVA

O erro é tratar NIS2 e CRA como temas separados.

A pressão regulatória está a empurrar as empresas para uma só lógica. Governance, produto, cadeia de fornecimento e resposta a incidentes.

NIS2

Impõe governação, gestão de risco, reporte de incidentes e maior exposição da gestão de topo.

CRA

Leva segurança para o ciclo de vida do produto digital: desenho, vulnerabilidades, atualizações e evidência.

Resultado prático

A organização deixa de poder separar compliance, segurança, procurement e produto como se fossem quatro conversas diferentes.

Risco real

Ter controlos dispersos e documentação avulsa, mas sem arquitetura integrada de responsabilidade.

Leitura correta

A questão já não é apenas técnica, mas sim de resiliência operacional e capacidade de permanecer defensável.

NIS2

O que a NIS2 muda na prática

A diretiva não é apenas mais um tema de IT.

1. Board exposure

A gestão de topo deixa de poder alegar distância operacional pois há deveres de supervisão, decisão e evidência.

2. Incidentes com mais peso

O valor do reporte vai para além da rapidez. Está na maturidade do processo, nos critérios e na cadeia de escalonamento.

3. Third-party risk

Serviços críticos, cloud, software, OT e dependências externas entram no perímetro da conversa.

4. Documentação

Sem análise de âmbito, responsabilidades definidas e evidência de decisão, a organização entra no regime já em défice.

CRA

O que o Cyber Resilience Act muda para produtos digitais

O CRA desloca a segurança para o desenho, desenvolvimento, manutenção e vigilância pós-colocação no mercado.

Segurança por desenho

É preciso demonstrar requisitos de segurança incorporados desde o início, não basta corrigir depois.

Vulnerabilidades

A gestão de vulnerabilidades e o regime de atualização passam a ser parte da responsabilidade do produto.

Cadeia de valor

Fabricantes, importadores e distribuidores deixam de poder tratar a segurança como assunto de outro interveniente.

Evidência

Sem documentação, testes, governance e critérios de decisão, a conformidade torna-se frágil mesmo antes de fiscalização.

Leitura dura

O CRA não é apenas uma obrigação técnica. É uma mudança de modelo sobre quem assume risco quando o produto falha.

ONDE MUITAS EMPRESAS FALHAM

A fragmentação continua a ser o problema problema central.

Os requisitos multiplicam-se, mas o erro continua a ser organizacional.

Segurança isolada

A equipa técnica trabalha sozinha e o jurídico aparece tarde demais.

Procurement cego

Contrata-se software e cloud sem mapear obrigações, dependências e segurança contratual.

Produto sem governance

Desenvolvimento e roadmap avançam sem matriz clara de responsabilidade regulatória.

Incidentes sem disciplina

Há playbooks técnicos, mas não há critérios consistentes de escalonamento, prova e accountability.

Consequência

No papel parece haver trabalho feito, mas na prática, há uma organização com controlos dispersos e exposição mal governada.

O QUE FAZER AGORA

Quick Wins - Cinco ações com valor imediato imediato

Não é um exercício para “mais tarde”,é um tema de arquitetura de controlo.

1. Rever o âmbito

Confirmar serviços, entidades, produtos e dependências que entram na discussão.

2. Unir legal + segurança + produto

Sem esta tríade, a resposta nasce partida.

3. Mapear fornecedores críticos

Cloud, software, OT, managed services e fabricantes.

4. Criar evidência

Critérios de decisão, atas, responsabilidades, playbooks e métricas.

5. Tratar isto como governance

Se fica só em IT, a organização já começou mal.

CONCLUSÃO

A nova pergunta não é “quem “quem trata da segurança?”. segurança?”.

A pergunta séria é
- Como é que a organização governa segurança, produto, terceiros e responsabilidade regulatória como um só sistema?

Se a discussão ainda está em silos, a execução já está atrasada.

AHKORIS | Driven by ethics. Building compliance.