

O País das Brechas: A Ciberfragilidade de um Estado Desprotegido

Publicado em 2025-05-02 13:18:18



Num tempo em que a guerra se faz por cabos de fibra e algoritmos silenciosos, Portugal continua a confiar num escudo de papel. As nossas infraestruturas tecnológicas, tanto públicas como privadas, estão repletas de brechas — algumas visíveis, outras escondidas sob camadas de ignorância institucional e arrogância técnica.

Demasiado jovem, demasiado fraco

As equipas técnicas em muitas entidades públicas são compostas por jovens recém-saídos das universidades ou cursos técnicos acelerados. Têm energia, mas falta-lhes contexto. Sabem instalar pacotes, mas não compreendem as camadas invisíveis do risco. Sem mentores experientes a seu

lado, são como aprendizes a pilotar aviões em zonas de guerra com apenas um manual de instruções.

O mercado valoriza o “dev rápido”, não o “engenheiro resiliente”. E assim se entregam sistemas críticos a quem ainda não teve tempo de falhar, aprender, afinar.

Público ou privado: o risco é comum

Hospitais, tribunais, escolas, autarquias, operadoras, bancos — todos vivem ligados por uma malha digital de confiança implícita. Basta uma falha. Um email inocente. Um acesso não revogado. Um servidor esquecido. E todo o edifício pode ruir.

O setor privado, por sua vez, subcontrata segurança a empresas que entregam firewalls como se fossem extintores: penduram na parede e esquecem. A cloud é usada como fuga para a frente. A cultura digital é superficial. O plano de contingência? “Esperar que não aconteça”.

O problema não é técnico. É civilizacional.

É o desprezo pelo saber acumulado. É o desinvestimento contínuo em quem tem 20, 30, 40 anos de estrada. É o culto da startup sem fundações, do improviso sem revisão.

Portugal precisa de um **Plano Nacional de Maturidade Digital** — não apenas para as máquinas, mas para as mentes.

Propostas para um novo paradigma

1. Mentores tecnológicos em cada estrutura crítica

Técnicos seniores devem ser colocados ao lado das novas gerações. Não como chefes. Como guias.

2. Auditorias obrigatórias de cibersegurança

A nível local, regional e nacional. Com relatórios públicos.

3. Criação de um selo de maturidade digital

Para premiar instituições que investem em boas práticas, planeamento e formação.

4. Programa de formação cruzada

Gestores aprendem o básico técnico. Técnicos compreendem o impacto estratégico. Um país digital exige transversalidade.

5. Sensibilização contínua

Através de **workshops, campanhas e simulações**. Porque a segurança é uma cultura, não uma configuração.

Conclusão: o tempo é agora

Não esperemos pelo próximo ataque para agir. Não façamos da fragilidade uma identidade. Portugal precisa de soberania digital, maturidade tecnológica e pensamento estratégico.

A liberdade de um país também se mede pela sua capacidade de **proteger os seus sistemas, os seus dados e o seu povo**.

Por : [Francisco Gonçalves](#)

in Fragmentos do Caos

Visita a Biblioteca de Fragmentos