Bruno Castro

Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

Agilidade e Segurança *by Design*

As empresas que ambicionam agilidade e inovação orientam hoje a sua estratégia em três vetores: governação integrada, modernização e segurança proativa. Este paradigma redefine a ambição de transformar uma organização tecnológica, onde cada componente, desde a cultura até à operação, é moldado pela tecnologia e pela conformidade normativa.

No centro desta transformação está o conceito de *governance by design*: em vez de tratar a segurança e a conformidade como etapas que sucedem ao desenvolvimento, estes elementos são incorporados desde a conceção dos processos e produtos.

A modernização da infraestrutura empresarial está a deixar de ser uma atualização pontual para se tornar num processo contínuo. Em 2025, as organizações mais ágeis tratam a infraestrutura como um ecossistema vivo, capaz de se adaptar a novas cargas de trabalho, requisitos regulatórios e oportunidades de negócio. O modelo híbrido e *multicloud* domina: aplicações críticas permanecem em *datacenters* privados, onde latência, soberania de dados e custos são mais controláveis, e enquanto *workloads* mais variáveis ou de IA intensiva aproveitam a elasticidade da *cloud* pública. Ferramentas de *orchestration* e *cloud management platforms* permitem gerir este ecossistema de ambientes como se fosse um só, garantindo segurança consistente e visibilidade total.

Em paralelo, a Inteligência Artificial (IA) deixa de ser uma simples ferramenta de apoio para se converter como impulsionadora da agilidade técnica e operacional ao automatizar deteção de anomalias, responder a incidentes e analisar milhões de registos de segurança em tempo recorde. Assim, a produtividade cresce, exigindo novos papéis, e uma cultura de melhoria contínua para suprimir os desafios adjacentes à utilização de IA. A eficácia destes sistemas depende da boa governação de dados e do ciclo completo de vida dos modelos (do treino à produção), permitindo cumprir requisitos de explicabilidade e mitigação de risco.

Relativamente à segurança proativa, um *Security Operations Center* (SOC) confere também uma enorme vantagem às empresas, quer em termos de defesa, mas também de conformidade, uma vez que um SOC surge como a pedra angular na resposta a regulamentações como a NIS2. As normas europeias relativas à cibersegurança exigem monitorização contínua, gestão de incidentes, comunicação rápida e responsabilização da liderança executiva sobre práticas de segurança (gestão de topo). Um SOC implementa estas capacidades de forma imediata, com especial relevância para as PME e organizações com recursos limitados. Na realidade portuguesa, o desafio é significativo e um SOC proporciona uma solução acessível para acelerar a conformidade, complementando ainda o *governance by design* ao garantir uma resposta imediata e adequada às exigências de segurança. A empresa ágil em 2025 não é a que corre mais, é a que aprende mais rápido, com tecnologia, dados e governação, a caminharem todos na mesma direção.

> «A modernização da infraestrutura empresarial está a deixar de ser uma atualização pontual para se tornar num processo contínuo.»