Por uma Doutrina Proativa 360º de Cibersegurança e Resiliência

— *Potenciais Contribuições de IA* —

José A. S. Alegria

Redshift Board Advisor
CIIWA Ambassador and Strategy Advisor
Former Chief Security Officer & CISO, Altice Portugal
Former Worldwide Coordinator for the CyberWatch Program, Altice Group
Membro fundador do Colégio de Engª Informática da Ordem dos Engenheiros e
Membro do Comité de Admissão e Qualificação (CAQ) da Ordem dos Engenheiros
Former Advisor, European Cybercrime Center

1 de abril de 2026

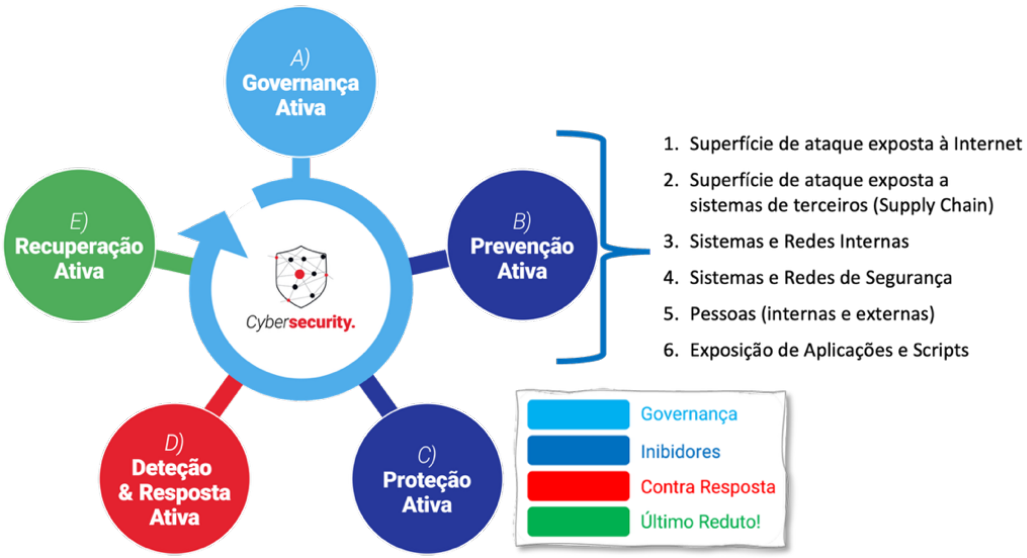
Resumo

Numa era marcada pelo crescimento de ameaças no ciberespaço, especialmente em termos de ataques de **RANSOMWARE** cada vez mais sofisticados e potencialmente catastróficos, é fundamental garantir estratégias proativas de ciber defesa de modo a proteger uma organização face a esses riscos. Nesta apresentação irei abordar uma **Doutrina Proativa de Ciber Segurança e Resiliência** que tenho vindo a desenvolver desde o ataque do **RANSOMWARE WannaCry**, em 12 de maio de 2017, e que desde então tenho expandido e aplicado com bastante sucesso enquanto **CISO** (*Chief Information Security Officer*) de grandes empresas.

Uma estratégia moderna de cibersegurança não se deve limitar a modelos tradicionais estáticos e reativos, que são atualizados a cada dois ou três anos, i.e., tipicamente com demasiado atraso face à rápida evolução das ameaças. Deve sim favorecer uma alternativa mais holística, contínua, dinâmica, proativa, suportada numa sólida análise situacional com base em métricas objetivas e confiáveis.

A doutrina que criámos não se restringe apenas a um conjunto de orientações ou protocolos. Representa uma mudança de paradigma na governança da cibersegurança, na sua melhoria contínua, com foco em lidar com ataques potencialmente catastróficos, integrando cinco dimensões estratégicas, nomeadamente: **A) Governança Ativa**, **B) Prevenção Ativa**, **C) Proteção Ativa**, **D) Deteção e Contrarresposta Ativa** e, finalmente, **E) Recuperação Ativa**. Todas necessárias! Todas proativas! Nenhuma é por si só suficiente. E todas têm de ser geridas ("*governadas*") continuamente, proactivamente, de forma coordenada e holística (360º), e com forte suporte de uma análise situacional baseada em métricas objetivas e confiáveis, e com suporte racional de agentes de suporte baseados em tecnologias de IA.

A dimensão "***B)* Prevenção Ativa**", que visa **inibir** a oportunidade de um ataque sequer se materializar, inclui, por sua vez, 6 subdimensões, cobrindo as várias superfícies de ataque e ativos: 1) exposição à Internet, 2) exposição a ativos de terceiros ("*supply-chain*"), 3) ativos internos, 4) ativos da própria arquitetura de segurança, 5) pessoas (internas e externas), e, finalmente, 6) exposição de aplicações e scripts.



Nesta apresentação irei descrever a doutrina em termos gerais e abordar alguns desafios e oportunidades em termos de investigação e desenvolvimento: análise situacional racional, métricas relevantes, e automação inteligente dos principais processos associados à governança da doutrina.

Cybersecurity.
Security is a Team effort, starting with You!
But always under Proactive Governance!