Ransomware não é um incidente de TI, é uma crise de negócio.

Estratégias de Continuidade e Orquestração para a Alta Liderança

Heloisa Diniz

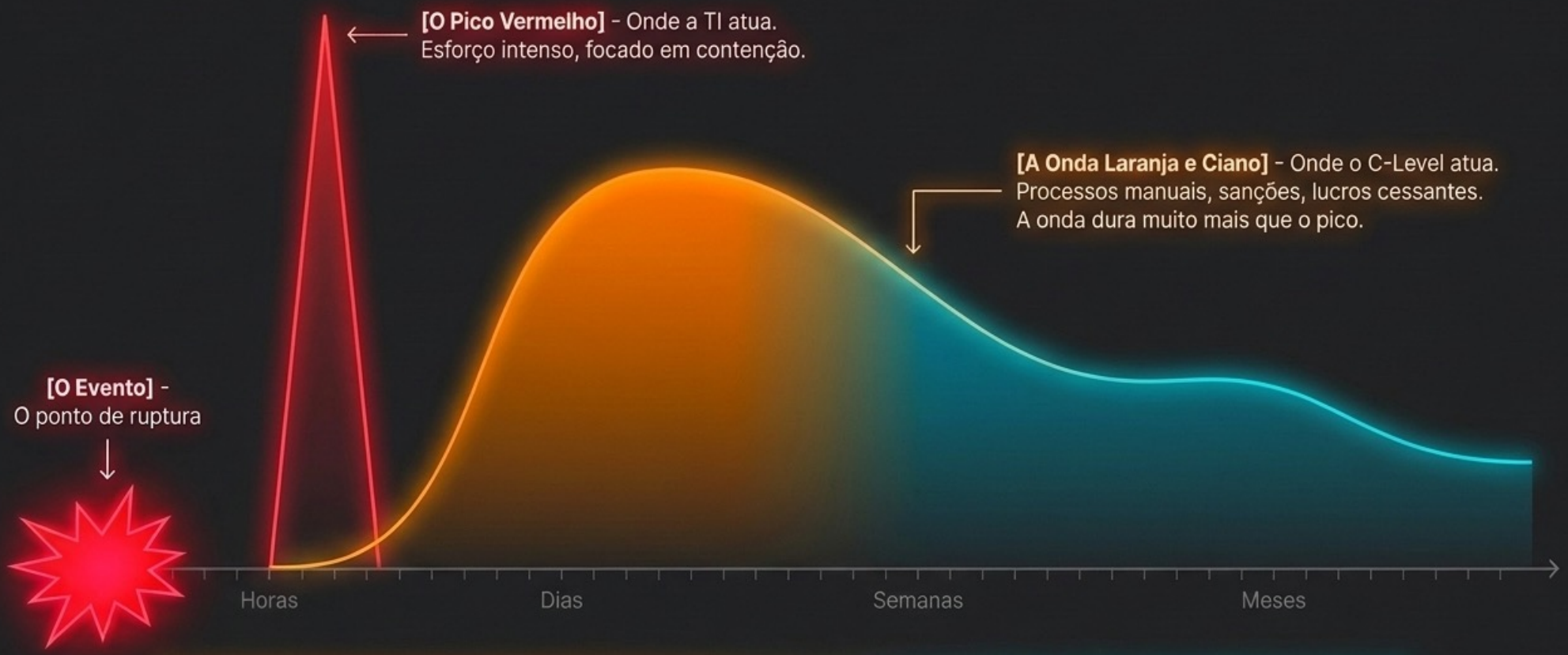
APCRS • Cyber Executive Day • Visão Estratégica para o C-Level

A quebra de paradigma: Onde a batalha é realmente perdida.

A Ilusão (O "Problema de TI")		A Realidade (A Crise de Negócio)	
Foco Principal	Isolar o malware e restaurar servidores.	**Foco Principal**	Manter a operação crítica, proteger o caixa e a reputação.
Duração Típica	Horas a dias (Pico técnico agudo).	**Duração Típica**	Semanas a meses (Onda de choque persistente).
Comunicação	Silêncio enquanto a equipe técnica trabalha.	**Comunicação**	Gestão proativa de mídia, reguladores e clientes.
Liderança	O CISO atua de forma isolada no SOC.	**Liderança**	O CEO, CFO e Conselho orquestram a resposta.

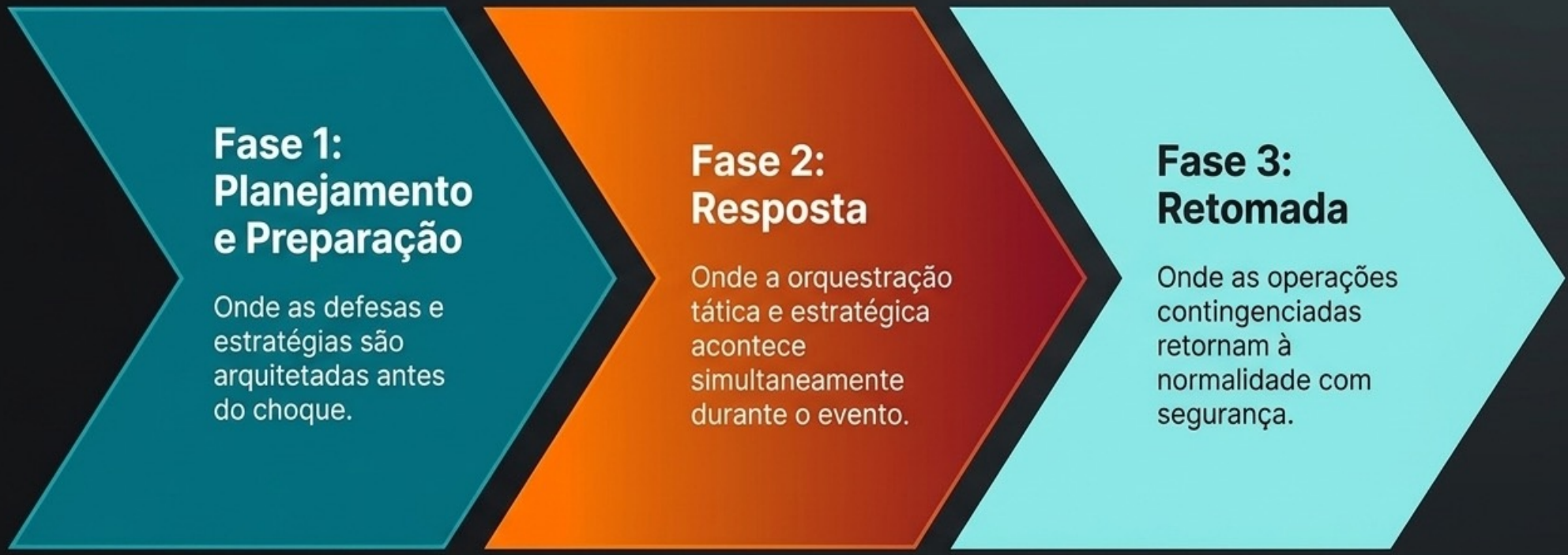
O C-level não pode delegar e esquecer. A tecnologia recupera os dados; a liderança recupera a confiança da empresa.

A anatomia de um ataque: O pico técnico e a onda estratégica.



A ilusão de que o problema acaba quando o servidor volta ao ar é o maior risco estratégico de uma organização. **A gestão da crise de negócios sobrevive muito além da resposta técnica**.

O framework executivo para a sobrevivência corporativa



Sobreviver a um ataque não é questão de improviso heroico, mas da execução rigorosa deste ciclo de vida institucional.

Mapeamento estratégico: Traduzindo bits em impacto financeiro.

Análise de Risco de Continuidade

Identificação de cenários críticos e ameaças (como ransomware) que têm o potencial real de paralisar a esteira de de valor da companhia.

Business Impact Analysis (BIA)

A bússola do executivo. Define o RTO (Recovery Time Objective) não pelo que a TI quer, mas pelo que o caixa da empresa suporta antes de danos irreversíveis. Determina quais processos sangram dinheiro mais rápido e ditam a prioridade matemática de recuperação.

A arquitetura de resposta:
Múltiplos planos, uma única orquestração.

Plano de Emergência (PE)

- **Foco**: Segurança imediata.
- **Ação**: Primeiros socorros e contenção primária.

Plano de Continuidade dos Negócios (PCN)

- **Foco**: O Negócio.
- **Ação**: Processos contingenciados (trabalho manual) para sobrevivência.
- **Dono**: Diretorias de Negócio.

Plano de Gestão de Crise (PC)

- **Foco**: Reputação e Regulamentação.
- **Ação**: Coordenação C-level, comunicação externa, decisões jurídicas.
- **Dono**: Comitê de Crise (C-Level).

Plano de Recuperação de Desastres (DRP)

- **Foco**: A Tecnologia.
- **Ação**: Reconstrução segura do ambiente de TI e restauração de dados.
- **Dono**: TI / Segurança da Informação.

A verdadeira arena do C-Level: O início da Gestão de Crise.

A decisão estratégica de proteger o amanhã.

> “A segurança digital deixou de ser uma preocupação técnica e tornou-se a decisão de negócio mais crítica da nossa década.”

1. Governança Ativa

Cobrar do seu CISO os planos de Continuidade e BIA aprovados, não apenas relatórios técnicos de antivírus bloqueados.

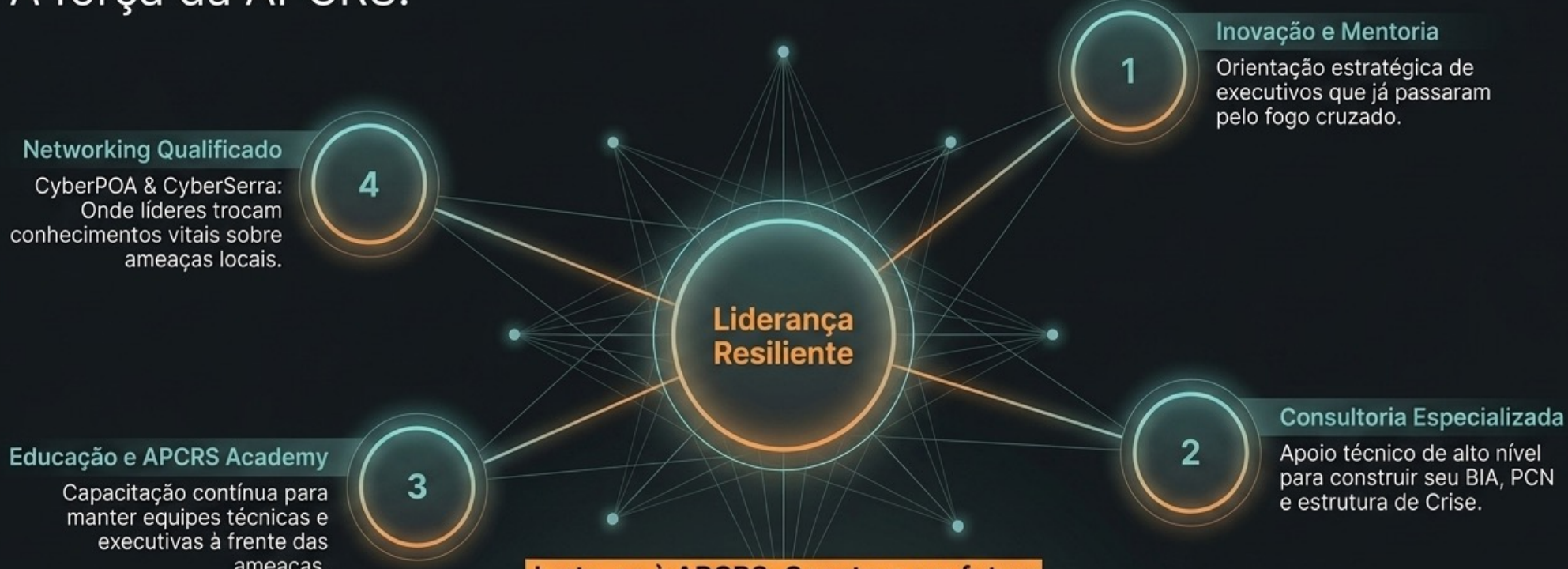
2. Cultura de Simulação

Participar pessoalmente dos **exercícios de mesa** (Tabletop Exercises). A primeira vez que sua diretoria se reúne para uma crise não pode ser durante um ataque real.

3. Apetite ao Risco Claro

Financiar a resiliência **adequadamente**, entendendo **matematicamente** o impacto financeiro exato de um dia de fábrica parada.

Você não precisa desenhar este mapa sozinho.
A força da APCRS.



Junte-se à APCRS. Construa um futuro digital seguro, orquestrado e na verdadeira linguagem de negócios.