WHITEPAPER

Como apresentar o orçamento de cibersegurança ao conselho

Um método para transformar a reunião de orçamento em uma decisão de apetite de risco, com números que a diretoria consegue defender.

SÉRIE	EDIÇÃO	PÁGINAS	PÚBLICO
Decisão executiva	Junho 2026	6	CISOs, CFOs e conselheiros

SUMÁRIO EXECUTIVO

O orçamento de segurança não é aprovado quando o CISO prova que as ameaças são graves. Ele é aprovado quando o conselho entende qual risco está comprando ao dizer não.

A maioria das apresentações de orçamento de cibersegurança falha por um motivo simples: ela responde à pergunta errada. O CISO chega com inventário de ferramentas, contagem de vulnerabilidades e siglas. O conselho quer saber outra coisa: quanto custa, o que isso reduz e o que acontece se não aprovarmos. Este whitepaper propõe um método em quatro movimentos para reposicionar a conversa: traduzir o orçamento em blocos de decisão, ancorar o pedido em redução mensurável de exposição, apresentar cenários em vez de um número único e fechar com uma pergunta de apetite de risco, não com um pedido de verba.

8–12%
do orçamento de TI é a faixa de referência de gasto em segurança para empresas maduras
`benchmark setorial · ver §3`

3 cenários
é o formato que desloca a decisão de 'aprovar verba' para 'escolher exposição'
`método LATAMSEC · §4`

1 pergunta
deve encerrar a apresentação: qual nível de risco residual o conselho aceita assinar
`estrutura de fechamento · §5`

1 Por que o orçamento de segurança trava no conselho

Conselhos não rejeitam segurança. Rejeitam pedidos que não conseguem comparar com as demais decisões da pauta. Quando a expansão comercial chega com projeção de receita e o orçamento de segurança chega com uma lista de ferramentas, a comparação é impossível e a verba vira despesa discricionária: a primeira a ser cortada.

Há três padrões recorrentes nas apresentações que travam. O primeiro é o vocabulário: EDR, SIEM, lateral movement e CVE não significam nada para quem decide alocação de capital. O segundo é a ausência de linha de base: sem um score de maturidade medido, o conselho não tem como saber se o investimento anterior produziu efeito. O terceiro é o medo como argumento. Manchetes de ataques a terceiros geram desconforto por dez minutos e ceticismo no ano seguinte, quando o ataque previsto não aconteceu.

> REGRA DE OURO
> Teste rápido antes da reunião: se cada slide não responde a **o que pode dar errado**, **quanto custa se der** ou **quanto este investimento reduz dessa conta**, o slide está falando com a pessoa errada.

2 Reorganize o pedido em cinco blocos de decisão

Um número único ("precisamos de R$ 14 milhões") convida ao corte percentual. Cinco blocos com naturezas distintas convidam à decisão informada, porque cada bloco tem uma consequência diferente quando cortado.

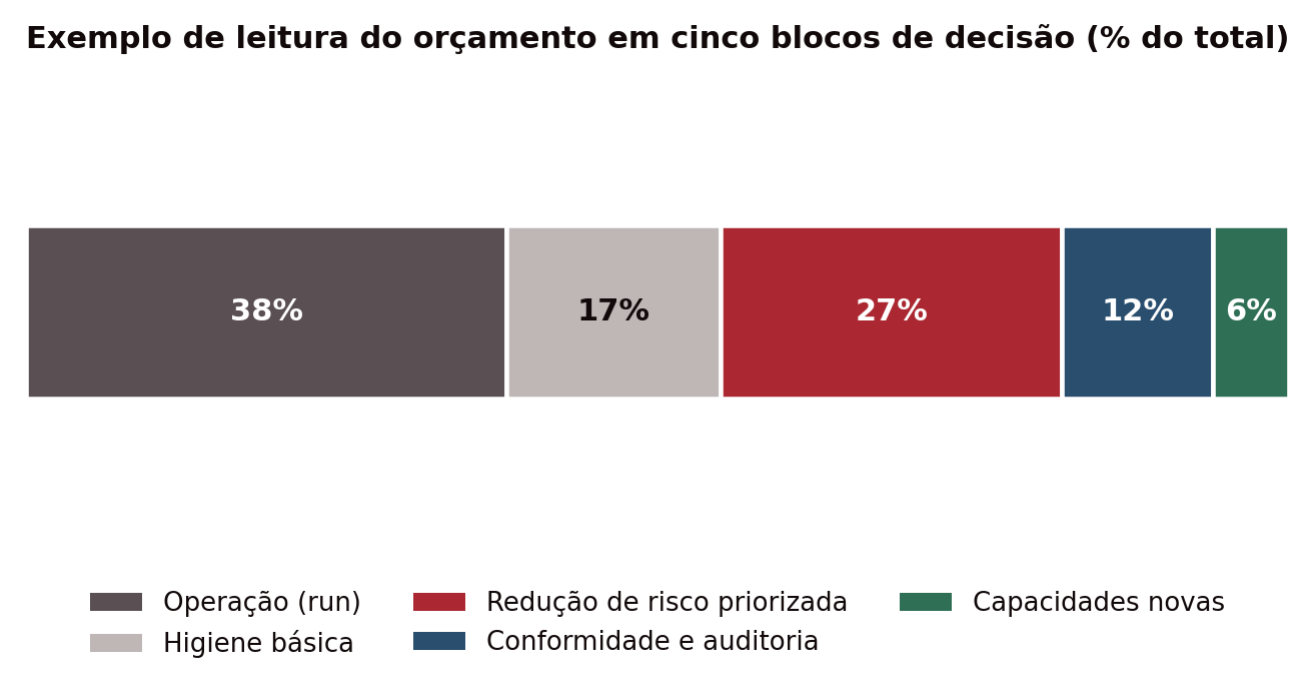

Figura 1 · Distribuição ilustrativa. As proporções variam por setor e maturidade; a estrutura de leitura, não.

BLOCO	O QUE COBRE	O QUE SIGNIFICA CORTAR
Operação (run)	Licenças, SOC, MDR, time, contratos vigentes que sustentam a proteção atual.	Desligar proteção que já funciona. Corte aqui é regressão, não economia.
Higiene básica	Patching, backup testado, MFA, hardening, gestão de identidades.	Aceitar exposição a ataques de oportunidade, os mais frequentes e baratos de explorar.
Redução de risco priorizada	Projetos que atacam os maiores riscos do registro corporativo, ranqueados por impacto.	Manter conscientemente os riscos do topo da lista. Deve ser decisão registrada em ata.
Conformidade e auditoria	LGPD, exigências setoriais, certificações exigidas por clientes e contratos.	Multa, perda de contrato ou bloqueio comercial. Em geral é o bloco menos negociável.
Capacidades novas	Segurança para novas frentes do negócio: nuvem, IA, expansão internacional.	Adiar proteção de iniciativas que a própria diretoria aprovou. Incoerência estratégica.

3 Ancore em números que sobrevivem a perguntas

O conselho confia em tendência medida, não em adjetivo. Três famílias de números sustentam um pedido de orçamento: a evolução do score de maturidade ao longo do tempo, os indicadores operacionais que provam capacidade de execução (tempo de detecção e de resposta, taxa de remediação de vulnerabilidades críticas dentro do prazo) e a comparação com a faixa de investimento do setor. Sobre esta última: a referência usual de mercado situa o gasto com segurança entre 8% e 12% do orçamento de TI. Estar fora da faixa não é argumento sozinho, mas estar muito abaixo dela com incidentes em alta é um fato difícil de ignorar.

Evite a precisão falsa. Dizer "há 73% de chance de ransomware" destrói credibilidade na primeira pergunta. Faixas honestas funcionam melhor: "um incidente de indisponibilidade de um dia custaria entre R$ 2 e 4 milhões em receita parada, antes de multa e dano reputacional". Quando a empresa adota um método de quantificação como FAIR, as faixas ganham rastreabilidade; quando não adota, faixas conservadoras documentadas já bastam para a conversa.

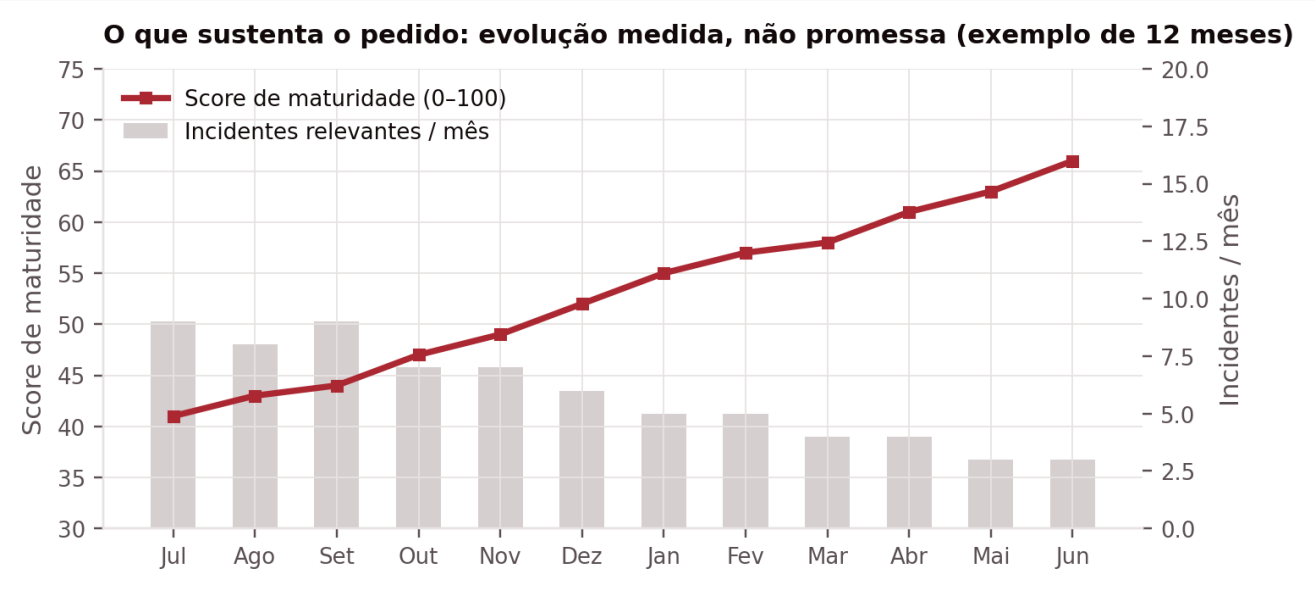

Figura 2 · O gráfico que abre a reunião: maturidade subindo, incidentes caindo. Investimento passado virou resultado medido.

4 Apresente cenários, não um número

O movimento que muda a natureza da reunião: em vez de defender um valor, apresente três pacotes e o risco residual de cada um. O cenário A mantém o orçamento atual e descreve, por escrito, quais riscos do registro permanecem abertos. O cenário B cobre operação, higiene e conformidade, e trata só os dois ou três riscos mais críticos. O cenário C é o plano recomendado, com a curva completa de redução de exposição. A partir daí o conselho não está mais aprovando uma verba: está escolhendo um ponto na curva.

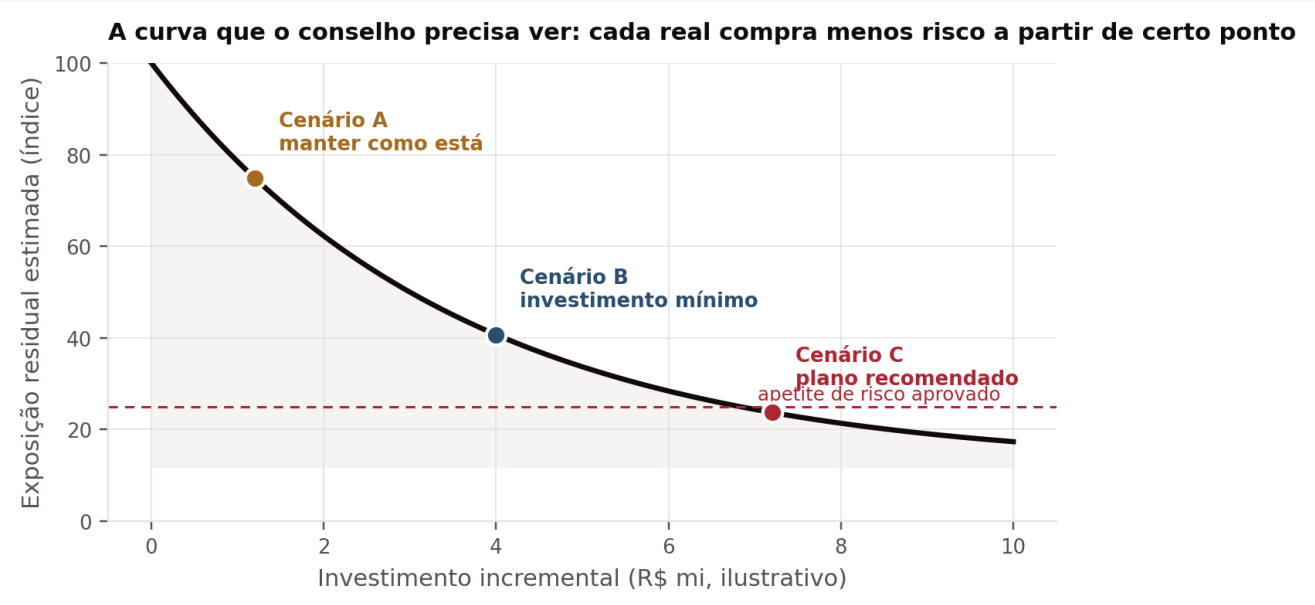

Figura 3 · Curva de exposição residual por investimento. O ponto de inflexão mostra onde o retorno marginal cai, um argumento que protege o CISO tanto de pedir pouco quanto de pedir demais.

PROTEÇÃO DE GOVERNANÇA

Cenários têm um efeito colateral valioso: registram em ata que o risco do cenário escolhido foi apresentado e aceito. Se o incidente acontecer, a discussão deixa de ser "por que ninguém avisou" e passa a ser "o plano aprovado está sendo executado".

5 A estrutura da apresentação, slide a slide

SLIDE	CONTEÚDO	TEMPO
1 · Postura atual	Score de maturidade, tendência de 12 meses, uma frase de diagnóstico.	3 min
2 · O que o investimento anterior comprou	Resultados medidos do ciclo passado: indicadores antes e depois.	4 min
3 · Top 5 riscos	Riscos em linguagem de negócio, com seta de tendência e custo estimado em faixa.	5 min
4 · Os cinco blocos	Orçamento decomposto, com a consequência de cortar cada bloco.	5 min
5 · Três cenários	A curva risco x investimento e o risco residual de cada pacote.	6 min
6 · Pedido e pergunta	Recomendação objetiva e a pergunta de fechamento sobre apetite de risco.	2 min

A pergunta de fechamento merece ser dita exatamente assim: "dos três cenários, qual nível de risco residual o conselho está disposto a assinar?". Ela transfere a decisão para onde ela pertence e transforma o orçamento de segurança em ato formal de governança.

6 O que a LATAMSEC entrega nessa conversa

Tudo que este whitepaper descreve depende de uma coisa: dados organizados e atualizados. O LATAMSEC Cockpit mantém o score de maturidade recalculado continuamente, com a evolução histórica pronta para o slide 1. O módulo de risco ranqueia o registro corporativo por impacto e probabilidade, alimentando o slide 3 e os cenários. O LATAMSEC Reports gera o material executivo com a narrativa de decisão já estruturada, sustentada por evidências auditáveis em vez de planilhas coletadas na véspera. A reunião de orçamento deixa de ser um evento anual de preparação heroica e vira a leitura trimestral de uma plataforma que já estava medindo.