# Benchmark de Orçamento do CISO 2026

Como 300+ líderes estão financiando segurança — e como transformar gasto em redução real de risco


# O Cenário Atual: Investimento Cresce, Confiança Ainda Não

Nos últimos anos, o orçamento de cibersegurança deixou de ser "opcional". O que mudou agora é o tamanho do desafio: nuvem crescendo rápido, times gastando uma parte enorme do tempo com complexidade operacional, muitas ferramentas ao mesmo tempo, e a chegada da IA acelerando tanto a defesa quanto o ataque.

Este material traduz os principais insights do relatório "The 2026 CISO Budget Benchmark", baseado em uma pesquisa com mais de 300 líderes de cibersegurança, para uma linguagem simples e aplicável no planejamento de orçamento brasileiro.

O ponto central do relatório é direto: as empresas estão investindo mais, mas a confiança de que isso está reduzindo risco de verdade ainda não acompanha. A oportunidade para 2026 é amadurecer a forma de decidir e medir: menos "comprar mais", mais "provar impacto".

# Resumo Executivo: Os Números Que Importam

**53%**

**Gastam Acima de US$ 5M**

A maior concentração de orçamento anual fica entre US$ 5M e US$ 10M, com 17% acima de US$ 25M

**85%**

**Aumentaram Gastos**

Cresceram investimentos em segurança vs. ano anterior, e 88% esperam aumentar novamente

**56%**

**Dizem Não Ser Suficiente**

Mesmo com mais verba, afirmam que o gasto total não mitiga riscos adequadamente

A nuvem é o grande motor do orçamento: 85% aumentaram gasto com segurança em nuvem, e a nuvem é vista como o principal foco futuro. O principal "freio" de efetividade é complexidade da nuvem: 49% apontam isso como o maior inibidor de resultados. Ferramentas demais também preocupam: 58% operam mais de 25 ferramentas; 28% têm 50+; 13% têm 100+.

Para o próximo ciclo, as apostas são claras: automação (62% das organizações) e visibilidade (48%) lideram as prioridades de investimento.

# Capítulo 1: Orçamento "Mais com Mais" Muda a Cobrança

O estudo mostra que, na maioria das empresas, o orçamento não está encolhendo. Ele está crescendo — e isso muda fundamentalmente a conversa com diretoria e conselho. Quando existe verba, a expectativa vira resultado: redução de risco mensurável, menos incidentes críticos, mais resiliência operacional e mais previsibilidade nos processos de segurança.

Esta transformação exige uma nova postura do CISO. Não basta mais justificar investimentos com base em ameaças hipotéticas ou tendências de mercado. A liderança executiva espera demonstração clara de como cada real investido se traduz em proteção efetiva dos ativos críticos da organização.

### Defina Objetivos Anuais

Estabeleça 3–5 objetivos que conectem segurança ao negócio: disponibilidade, proteção de dados, continuidade operacional

### Priorize Riscos por Impacto

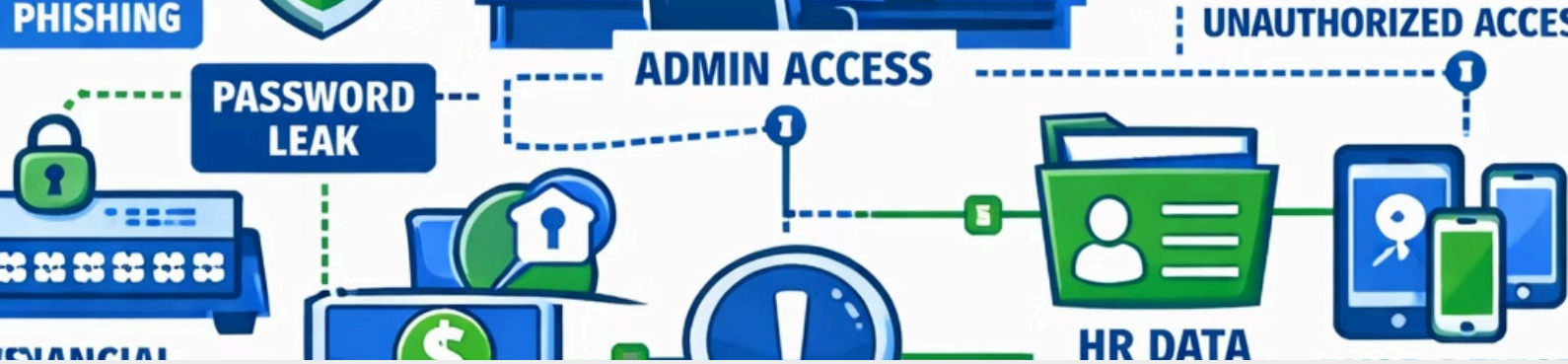
Transforme "listas de vulnerabilidades" em riscos priorizados com impacto real: LGPD, receita, operação

### Use Indicadores Executivos

Adote métricas que qualquer liderança entenda: tempo de correção de riscos críticos, cobertura de ativos, exposição de dados

**Ganhos esperados:** Mais apoio executivo, decisões mais rápidas e um orçamento defendido por impacto, não por medo. A segurança passa a ser vista como habilitadora do negócio, não apenas como centro de custo.

**Riscos associados:** Sem essa mudança de abordagem, o resultado é previsível: aumento de gasto sem redução proporcional de risco e questionamento recorrente de ROI. O orçamento pode até crescer, mas a credibilidade da área de segurança diminui.




# Capítulo 2: O Gap de Confiança — Investir Mais Não Basta

Mais da metade dos respondentes afirma que o investimento ainda não cobre o nível de ameaça percebido. Este dado revela um problema clássico e persistente: gasto não está virando confiança, porque falta priorização estratégica e prova tangível de efetividade.

A questão não é simplesmente aumentar o orçamento novamente. O desafio real é criar uma governança que transforme investimento em redução mensurável de risco. Isso exige formalizar o apetite a risco da organização — definir claramente o que é tolerável versus o que é inaceitável.

Um "mapa de risco" efetivo precisa unir múltiplas dimensões: criticidade do ativo, exposição atual, nível de privilégio de acesso e sensibilidade dos dados envolvidos. Apenas com essa visão integrada é possível estabelecer um framework de ROI de segurança que responda à pergunta fundamental: "quanto risco crítico foi realmente reduzido com esse investimento?"

**Ganhos esperados:** Menos discussões subjetivas e mais governança baseada em dados. Segurança vira decisão de gestão estratégica, não de urgência operacional. A confiança cresce quando há transparência sobre o que está sendo protegido e como.

**Riscos associados:** Crescimento contínuo de orçamento com sensação permanente de insuficiência, aumento de pressão sobre as equipes e desgaste progressivo do time de segurança. A frustração afeta tanto lideranças quanto profissionais técnicos.

# Capítulo 3: Pessoas e Serviços Gerenciados, O Maior Custo Exige Estratégia

O maior item do orçamento de cibersegurança é gente. Em média, pessoal interno e serviços gerenciados representam a fatia mais relevante do investimento total. Esta realidade torna essencial uma estratégia clara de como estruturar e otimizar esse investimento.

Sem estratégia definida, você paga caro e ainda assim sofre com falta de cobertura adequada, turn-over elevado e burnout das equipes. A escassez de profissionais qualificados no mercado brasileiro agrava ainda mais esse desafio, tornando cada contratação e cada parceria ainda mais críticas.

A chave está em separar claramente o que é núcleo estratégico interno — governança, gestão de risco, arquitetura de segurança, decisões de negócio — do que pode ser operado eficientemente por um parceiro de confiança, como monitoramento 24x7, triagem de alertas e resposta inicial a incidentes.

### Defina o Núcleo Estratégico

Mantenha internamente: governança, risco, arquitetura e decisões críticas de negócio

### Exija Transparência Total

Nada de "caixa-preta" com parceiros — visibilidade completa de processos, métricas e decisões

### Integre Processos

Crie fluxos integrados com TI/DevOps: correção, SLAs e priorização baseada em risco real

**Ganhos esperados:** Mais previsibilidade operacional, menos sobrecarga nas equipes internas e melhor retenção de talentos. Profissionais podem focar em trabalho estratégico em vez de operações repetitivas.

**Riscos associados:** Terceirização que não reduz complexidade, apenas muda o endereço do problema. Parceiros que não se integram aos processos da organização podem criar mais gargalos do que soluções.

# Capítulo 4: A Nuvem Consome o Time — E a Tendência Piora


### O Desafio da Escala

A nuvem cresce em velocidade e escala que processos manuais simplesmente não conseguem acompanhar

Em muitas organizações brasileiras, uma parte significativa do time de segurança está dedicada exclusivamente à nuvem — e esse foco tende a aumentar ainda mais nos próximos anos. O desafio é que a nuvem cresce em escala e velocidade exponenciais, enquanto processos manuais não conseguem acompanhar esse ritmo.

O resultado é previsível e prejudicial: fadiga das equipes, excesso de alertas que não podem ser todos analisados, e riscos críticos passando despercebidos em meio ao ruído operacional. A complexidade da multi-nuvem, com diferentes fornecedores e modelos de responsabilidade compartilhada, agrava ainda mais esse cenário.

01

### Inventário Automatizado

Implemente descoberta automática de ativos e contas em todas as nuvens — visibilidade vem antes de controle

02

### Padronize Tags e Classificação

Defina taxonomia clara: ambiente, dono, criticidade, tipo de dados processados

03

### Defina Responsabilidades

Estabeleça RACI claro entre Cloud/DevOps/AppSec/SecOps — sem sobreposição ou gaps

04

### Automatize Correções

Automatize remediações repetitivas e bloqueie apenas o que for realmente crítico — evite paralisar deploys

**Ganhos esperados:** Menos ruído operacional, mais foco no que realmente importa e maior resiliência operacional. Times conseguem ser proativos em vez de apenas reativos.

**Riscos associados:** Ambiente com pontos cegos críticos, correções lentas de configurações inadequadas e incidentes recorrentes por erros de configuração básicos que poderiam ser prevenidos.


# Capítulo 5: Alocação de Orçamento — Nuvem Lidera, Dados Crescem

O relatório mostra crescimento forte e consistente em categorias específicas como segurança de nuvem e segurança de dados. Esta tendência não é casual — é nessas camadas que mora grande parte do risco real enfrentado pelas organizações: exposição de dados sensíveis, permissões excessivas não auditadas e serviços mal configurados que criam portas abertas.

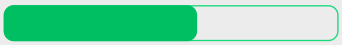
A questão estratégica é onde concentrar investimentos para máximo impacto. A recomendação é priorizar controles que reduzem risco de forma transversal: visibilidade ampla de ativos, gestão de postura de segurança, gestão robusta de identidade e acesso, e proteção efetiva de dados em repouso e em trânsito.

Evite a tentação de comprar ferramentas "pontuais" que resolvem problemas isolados sem integração com o ecossistema existente. Conecte sempre seus investimentos a requisitos de frameworks reconhecidos como ISO/IEC 27001:2022 e NIST CSF — cobrindo inventário, controle de acesso, detecção de anomalias e capacidade de resposta.

**Ganhos esperados:** Redução de desperdício financeiro, ganhos reais de eficiência operacional com automação e padronização de processos. Investimentos alinhados a frameworks facilitam auditorias e certificações.

**Riscos associados:** Gastos fragmentados onde cada área compra um pedaço da solução sem visão do todo. Resultado: ninguém enxerga o quadro completo de segurança, gaps críticos permanecem e a integração vira pesadelo.

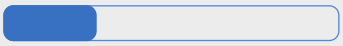
# Capítulo 6: Tool Sprawl — Mais Ferramenta Não É Mais Segurança



**58%**

### Operam 25+ Ferramentas

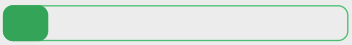
Mais da metade das organizações gerencia ao menos 25 soluções diferentes de segurança



**28%**

### Têm 50+ Soluções

Quase um terço lida com complexidade extrema de 50 ou mais ferramentas distintas



**13%**

### Chegam a 100+ Tools

Cenário crítico onde a quantidade de ferramentas cria mais problemas que soluções

Ferramentas se multiplicam rapidamente nas organizações. O estudo revela um cenário preocupante onde é comum encontrar ambientes com 25+, 50+ e até 100+ soluções de segurança convivendo simultaneamente. Este fenômeno, conhecido como "tool sprawl", tem consequências diretas e mensuráveis.

Muitas ferramentas criam problemas operacionais graves: custo de licenciamento e manutenção crescente, alertas duplicados que consomem tempo de análise, gaps de integração que impedem visão unificada, troca constante de contexto entre dashboards e baixíssima capacidade de priorização efetiva.

A solução exige disciplina. Faça um inventário real e honesto do stack tecnológico: o que existe, o que cada ferramenta realmente cobre, onde há sobreposição desnecessária. Corte baseado em três critérios objetivos: cobertura real de risco (não promessas), integração efetiva com processos existentes e redução de risco mensurável e comprovada. Consolide em plataformas quando possível, sempre mantendo governança clara e responsabilidade definida.

**Ganhos esperados:** Menos custo operacional total, mais visibilidade unificada do ambiente e capacidade de decisão mais rápida em incidentes. Analistas trabalham com eficiência em vez de lutarem contra ferramentas.

**Riscos associados:** "Ferramenta demais" inevitavelmente vira "risco demais": ninguém consegue ver o ataque completo, apenas fragmentos desconexos. Incidentes passam despercebidos porque a correlação entre sistemas é impossível.

# Capítulo 7: IA Muda o Jogo — Defesa e Ataque Acelerados

A pesquisa aponta investimento crescente em IA tanto para ganhar eficiência operacional quanto para lidar com ameaças impulsionadas por inteligência artificial. Mas também destaca riscos emergentes significativos ligados a modelos de linguagem e agentes autônomos com acesso a sistemas corporativos.

IA amplia dramaticamente escala e velocidade — tanto para defesa quanto para ataque. Quem não cria governança adequada agora inevitavelmente vai correr atrás depois de um incidente público e custoso. A janela para agir de forma preventiva está aberta, mas não ficará assim indefinidamente.

Crie controles mínimos essenciais para IA corporativa: inventário completo de modelos e fornecedores utilizados, avaliação estruturada de risco para cada caso de uso, proteção rigorosa dos dados usados no treinamento e inferência, monitoramento contínuo de acessos e permissões concedidas a sistemas de IA.


Trate "IA com acesso demais" como risco crítico de segurança — aplique rigorosamente o princípio de privilégio mínimo. Treine continuamente seus times sobre engenharia social moderna, que agora inclui ataques de phishing dramaticamente mais convincentes gerados por IA.

**Ganhos esperados:** Adoção mais segura e controlada de IA, redução drástica da chance de vazamento de dados proprietários, prevenção de acesso indevido via agentes autônomos e menos falhas de compliance com LGPD e GDPR.

**Riscos associados:** Exposição massiva de dados corporativos sensíveis, agentes com permissões excessivas causando danos, fragilidade crítica de governança que pode resultar em incidentes públicos e multas regulatórias pesadas.