

PESQUISA APCRS / MITI • 2026

# Riscos Digitais - Rio Grande do Sul

Exposição, maturidade e as decisões que cabem ao Conselho

---

Nycholas Szucko – Empreendedor, Conselheiro e Líder do LAB do MITI de Cibersegurança

# O estado opera com **maturidade C**

## Probabilidade de ataque bem-sucedido acima da média nacional

**50%**

**Maturidade RS 2026**

Brasil 2025: 58%

**56%**

**Probabilidade de ataque bem-sucedido**

Brasil 2025: 43%

**US\$ 1,31 mi**

**Impacto financeiro potencial**

Brasil 2025: US\$ 31,99 mi

- **Exposição concentrada em governança (69%) e terceiros (50%)**

São os dois únicos índices em faixa Alto e ambos estão fora do perímetro técnico.

- **Resiliência em 51%, a um ponto do nível crítico - Continuidade**

**A escala é invertida:** 0 a 50% é Crítico. Incidentes tendem a durar mais e custar mais.

- **Regulatório em 48%, a dois pontos da faixa Alto - Aplicador**

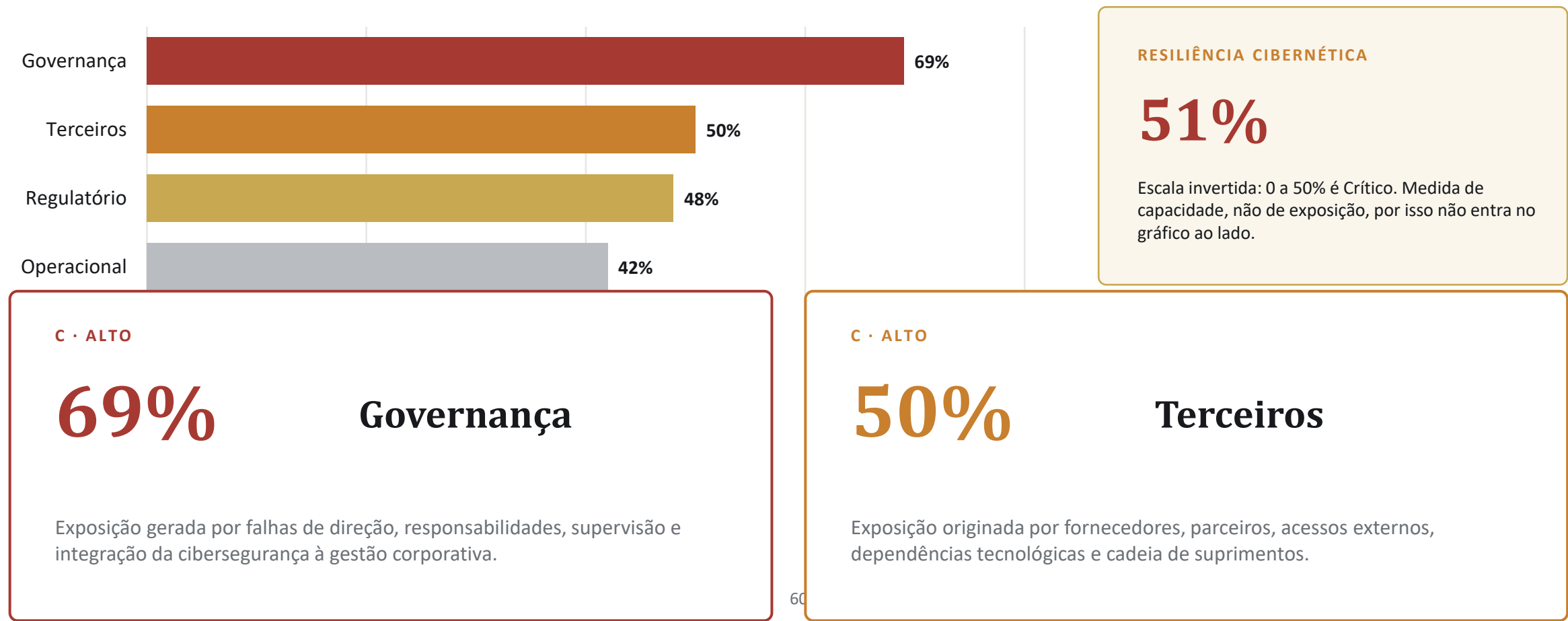
É o vetor com maior chance de reclassificação adversa no próximo ciclo.

- **Decisão central: apetite de risco e patrocínio executive - Bússola**

Duas decisões que custam apenas tempo do Conselho e destravam todo o roadmap.

# Oito dos nove índices são explicados por duas causas de governança

Índices de exposição do painel RS 2026. Quanto maior o valor, maior a exposição.



# A exposição já é material nas quatro dimensões pelas quais o Conselho responde



FINANCEIRA

**US\$ 1,31 mi**

Impacto potencial por empresa do painel. Perda esperada anualizada de US\$ 734 mil.



OPERACIONAL

**42%**

Índice em faixa Médio, agravado pela resiliência em 51%, que estende a duração da interrupção.



REGULATÓRIA

**48%**

A dois pontos da faixa Alto, com LGPD, ANPD e requisitos setoriais já em vigor.



REPUTACIONAL

**31%**

O menor índice do conjunto, porém fortemente correlacionado ao tempo de indisponibilidade.

As quatro dimensões compartilham a mesma raiz de governança, portanto respondem ao mesmo tratamento. Não são quatro programas, é um só.

# A exposição decorre de quatro lacunas estruturais, nenhuma delas tecnológica

CAUSA RAIZ

Cibersegurança não integrada à gestão corporativa · Índice de Governança em 69%

## QUATRO LACUNAS DE CONTROLE

1

### Apetite não definido

Não há nível de exposição aceito, formalizado e aprovado pelo Conselho.

2

### Patrocínio não nomeado

Não há responsável executivo designado nem rito de supervisão recorrente.

3

### Ecosistema não governado

Terceiros sem inventário, classificação por criticidade ou avaliação contínua.

4

### Recuperação não testada

Continuidade, resposta, backup e DR não validados em condição real.

## MANIFESTAÇÃO MEDIDA

50%

Terceiros

51%

Resiliência

48%

Regulatório

56%

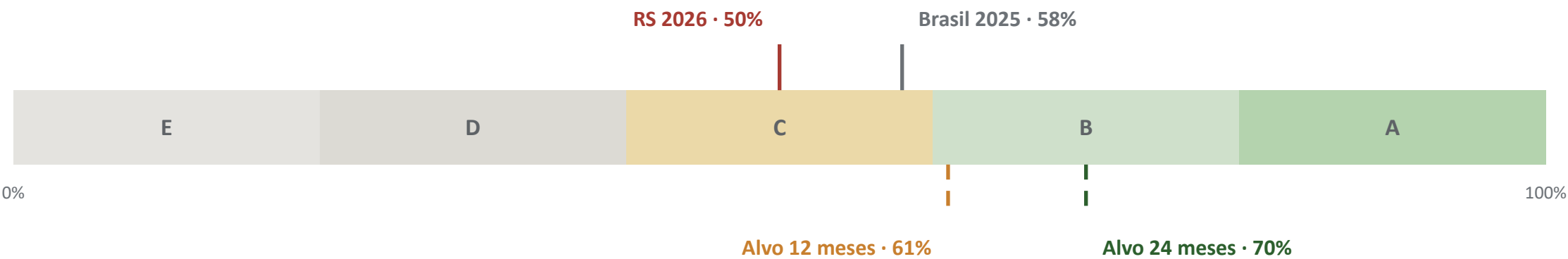
Ataque bem-sucedido

*Efeito combinado: a empresa não consegue provar o nível de controle que de fato pratica.*

# Jornada

## Sair da faixa C exige 11 pontos, um movimento realista em 12 meses

Faixa C: 41% a 60% · Faixa B: 61% a 80%



### Os 11 pontos iniciais

Vêm majoritariamente de governança e terceiros, os dois índices mais distantes do padrão de referência.

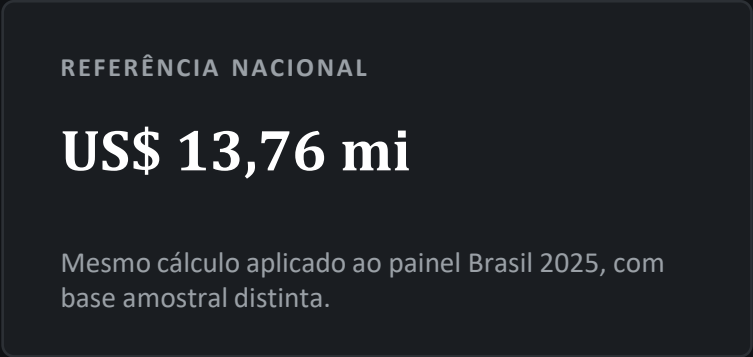
### Alvo de 12 meses

Entrada na faixa B, acima da média nacional de 2025. Depende apenas de decisões de governança.

### Alvo de 24 meses

Faixa B consolidada em 70%, com resiliência testada e programa de terceiros em operação.

# A inação custa aproximadamente US\$ 734 mil por ano em perda esperada



*Premissa declarada: o índice de 56% está sendo tratado como probabilidade em janela anual. Essa premissa precisa ser confirmada com a metodologia da pesquisa. Se a janela for maior, a perda esperada anual cai proporcionalmente e a prioridade de governança não muda.*

Empresa brasileira investem em media 5% do budget de TI em Cybersegurança

# Três horizontes levam o estado de 50% a 70% de maturidade

0 a 90 DIAS

## Contenção e validação

- Apetite de risco definido e aprovado
- Patrocínio executivo nomeado
- Inventário de terceiros críticos
- Teste real de restauração
- Lacunas de dados fechadas

**Marco de saída: apetite aprovado e inventário concluído**

3 A 12 MESES

## Fortalecimento

- Programa formal de riscos de terceiros
- Governança integrada à gestão corporativa
- Adequação regulatória documentada
- Controles e processos reforçados
- Primeiro ciclo de medição

**Marco de saída: maturidade em faixa B, 61% ou mais**

12 A 24 MESES

## Consolidação

- Continuidade e resposta testadas em exercício
- Automação de monitoramento e reporte
- Resiliência acima de 69%
- Melhoria contínua institucionalizada
- Maturidade em 70%

**Marco de saída: resiliência comprovada e reporte automatizado**

# Cinco quick wins de 0 a 90 dias endereçam as duas causas prioritárias

As duas primeiras iniciativas custam apenas tempo do Conselho e do CEO, e destravam todas as demais.

| Iniciativa                                          | Prioridade | Risco endereçado | Resultado esperado          | Responsável       | Dependência        | Indicador de sucesso            |
|-----------------------------------------------------|------------|------------------|-----------------------------|-------------------|--------------------|---------------------------------|
| Definir e aprovar apetite de risco digital          | Crítica    | Governança 69%   | Mandato formal do Conselho  | Conselho e CEO    | Nenhuma            | Documento aprovado em ata       |
| Nomear patrocinador executivo e rito trimestral     | Crítica    | Governança 69%   | Supervisão contínua         | CEO               | Apetite definido   | Rito realizado no trimestre     |
| Inventariar e classificar terceiros por criticidade | Alta       | Terceiros 50%    | Visibilidade do ecossistema | COO e Suprimentos | Patrocínio nomeado | 100% dos críticos mapeados      |
| Testar restauração de backup dos sistemas críticos  | Alta       | Resiliência 51%  | Capacidade comprovada       | TI                | Nenhuma            | RTO e RPO medidos em teste real |
| Validar as lacunas de dados da pesquisa             | Média      | Todos            | Base analítica confiável    | Risco             | Acesso ao painel   | Lacunas fechadas ou declaradas  |

As duas iniciativas críticas não têm custo financeiro Elevado, pessoas e processos e são pré-requisito das demais.

# Cinco iniciativas estruturantes consolidam a maturidade entre 3 e 24 meses

| Iniciativa                                             | Horizonte     | Risco endereçado | Resultado esperado                  | Responsável         | Indicador de sucesso             |
|--------------------------------------------------------|---------------|------------------|-------------------------------------|---------------------|----------------------------------|
| Programa formal de gestão de riscos de terceiros       | 3 a 12 meses  | Terceiros 50%    | Avaliação contínua dos críticos     | Risco e Suprimentos | Índice Terceiros abaixo de 40%   |
| Estrutura de governança integrada à gestão corporativa | 3 a 12 meses  | Governança 69%   | Cibersegurança na pauta do Conselho | CEO                 | Índice Governança abaixo de 55%  |
| Adequação regulatória documentada e auditável          | 3 a 12 meses  | Regulatório 48%  | Evidência de conformidade           | Jurídico e Risco    | Índice Regulatório abaixo de 40% |
| Plano de continuidade e resposta testado por exercício | 12 a 24 meses | Resiliência 51%  | Recuperação comprovada              | COO e TI            | Resiliência acima de 69%         |
| Automação de monitoramento e reporte executivo         | 12 a 24 meses | Todos os índices | Medição contínua                    | TI e Risco          | Painel mensal ativo              |

Todas as metas de índice são recomendação do autor e devem ser calibradas contra o apetite de risco aprovado pelo Conselho, maturidade da empresa e levado ao context da vertical de atuação de cada empresa.

# A supervisão só é efetiva com mandato, responsável nomeado e cadência fixa

|   |                           |                                                                              |
|---|---------------------------|------------------------------------------------------------------------------|
| ● | Conselho de Administração | Define o apetite, aprova o programa e recebe reporte trimestral.             |
| ● | CEO                       | Nomeia o patrocinador executivo e responde pela execução perante o Conselho. |
| ● | Patrocinador executivo    | Conduz o programa, remove obstáculos e reporta ao Conselho.                  |
| ● | Risco e TI                | Executam, medem e produzem a evidência auditável.                            |

CADÊNCIA

**Mensal**

Diretoria executiva

---

**Trimestral**

Conselho de Administração

---

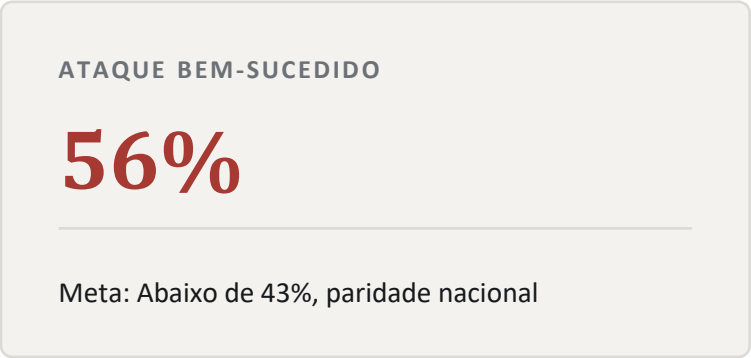
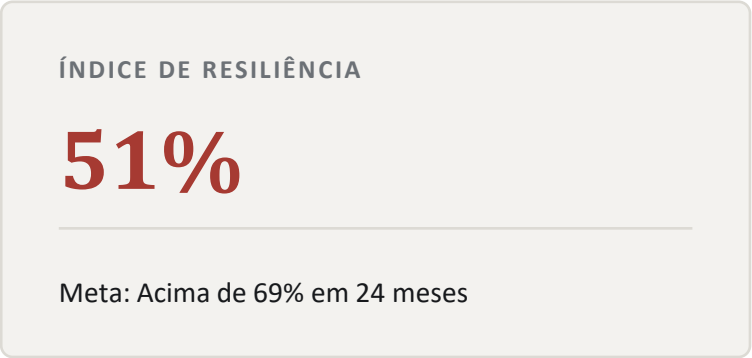
**Anual**

Revisão do apetite de risco

*Sem responsável nomeado e cadência fixa, o índice de Governança em 69% não se move, e com ele nenhum dos demais.*

# Seis indicadores traduzem exposição em linguagem de decisão

Valores atuais do painel RS 2026 e metas recomendadas para os horizontes de 12 e 24 meses.



# Quatro decisões do Conselho destravam todo o roadmap

1

**Aprovar o apetite de risco digital**

Nível de exposição que a organização aceita conviver, expresso nos índices da pesquisa.

**Conselho** · próxima reunião ordinária

2

**Nomear o patrocinador executivo e o rito de supervisão**

Quem responde pelo programa perante o Conselho e com que cadência reporta.

**CEO, com homologação do Conselho** · 30 dias

3

**Mandatar o programa de governança do ecossistema de terceiros**

Inventário, classificação por criticidade e avaliação contínua, com poder de veto contratual.

**Conselho, execução por COO e Suprimentos** · 90 dias

4

**Determinar teste real de recuperação nos sistemas críticos**

Comprovação de RTO e RPO medidos em exercício, não em documento.

**Conselho, execução por TI** · 90 dias