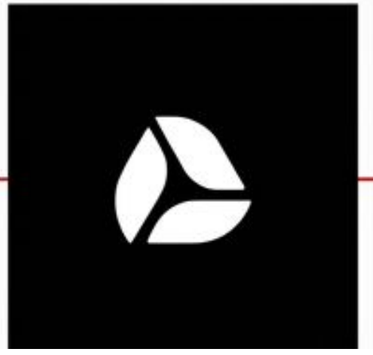
Como criar um modelo integrado de Riscos Cibernéticos com GRC.

Do relatório técnico à **decisão executiva:**
conectando vulnerabilidades, processos e planos de ação.

Uma parceria **risklab.** + **Perinity**

risklab.



perinity

Cyber só vira prioridade executiva quando deixa de ser vulnerabilidade técnica e aparece como risco de negócio.

risklab. + Perinity

perinity

Onde está o impacto no negócio?

Vulnerabilidades tratadas apenal por severidade técnica.

Controles Internos de segurança sem testes de efetividade.

Planos de ação vencidos sem escalonamento.

Relatórios que mostram volume, mas nenhuma prioridade corporativa.

O Relatório Técnico (Modelo Fraco)

Foco em volume: Temos 42 vulnerabilidades críticas.

Métricas baseadas em severidade CVSS, quantidade de patches pendentes, incidentes por incidentes por volume e backlog infinito de TI.

A Visão Executiva (Modelo Forte)

Foco em impacto: Quais destas 42 vulnerabilidades afetam processos críticos, expõem dados sensíveis, possuem Controles Internos ineficazes ou quebram obrigações regulatórias?

A gestão decide sobre impacto e continuidade, não sobre CVE.

A Arquitetura da Integração

Vulnerabilidade / Evento
O dado técnico bruto

Ativo Digital
O sistema ou servidor

Processo Crítico
A operação dependente

Risco Corporativo
A tradução para a matriz

Controles Internos
As barreiras e efetividades

A evolução não é misturar áreas, mas integrar informações mantendo a independência das linhas de defesa.

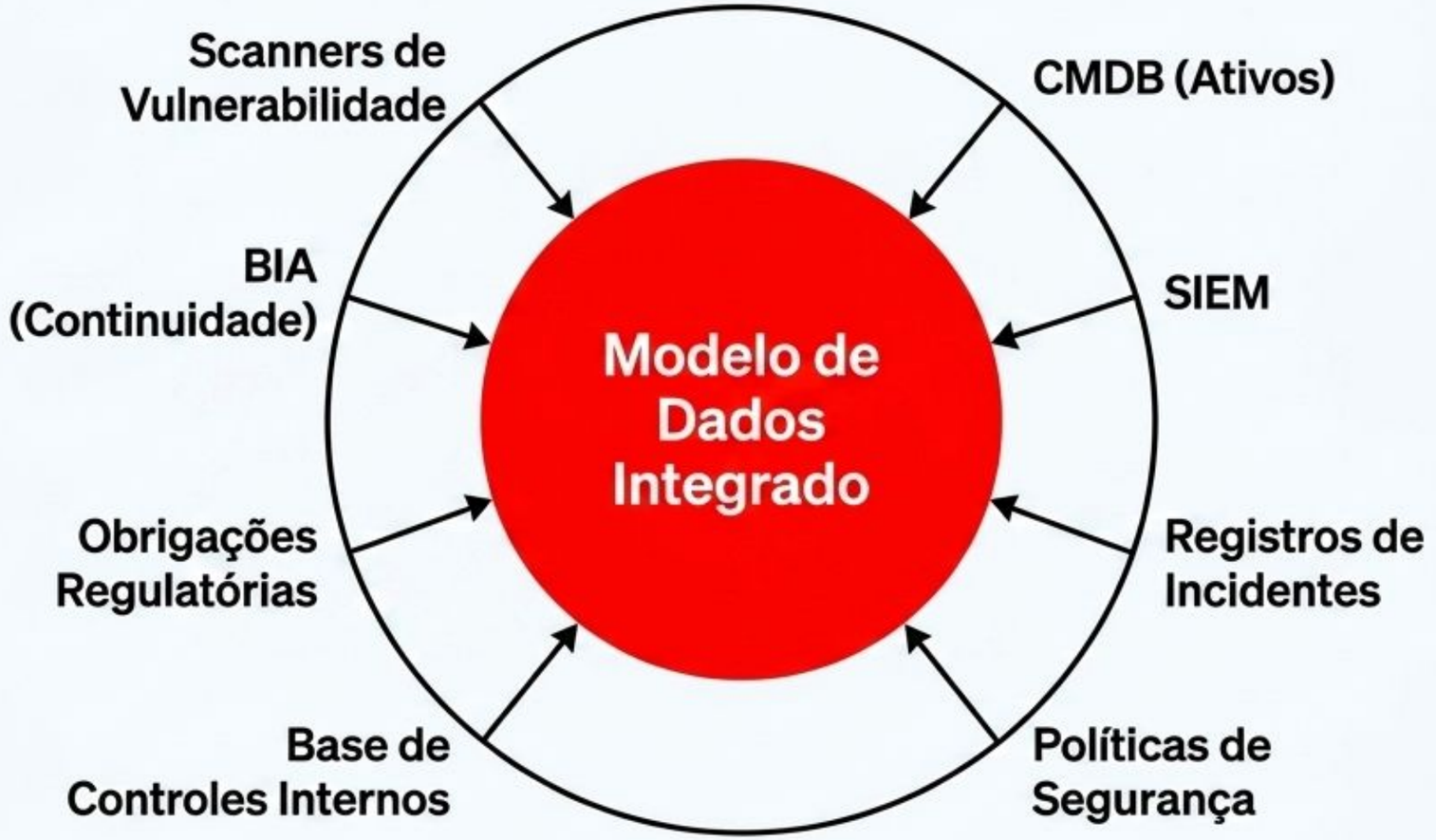
O Dicionário de Tradução Executiva

Vulnerabilidade Crítica em Servidor Core	→ Risco de Indisponibilidade de Sistemas Críticos
Backup Sem Teste de Restauração	→ Risco de Falha em Continuidade Tecnológica
Política de Acesso Vencida	→ Risco de Não Conformidade e Acesso Indevido

Taxonomia de Cyber Integrada ao GRC

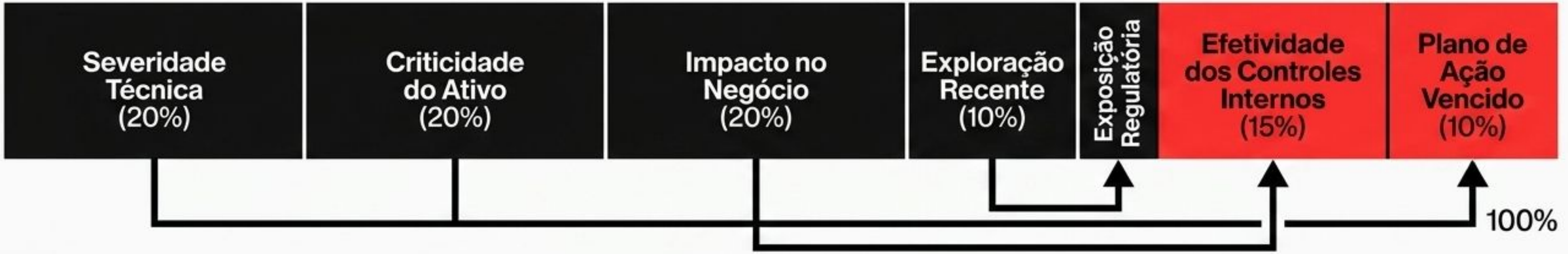
Risco de indisponibilidade de sistemas	**Risco de vazamento de dados (LGPD)**	Risco de fraude digital	**Risco de ransomware e extorsão**
Risco de terceiros tecnológicos	Risco de falha na gestão de acessos	Risco de perda de integridade de dados	Risco de falha em resposta a incidentes

O Motor de Dados



O valor do modelo reside no Monitoramento Contínuo destas fontes, garantindo que o risco reflita a realidade.

O Score ICR: Índice de Criticidade de Risco Cibernético



A Arquitetura do Dashboard Dashboard Executivo

1. Visão Executiva (Cards de Exposição)
2. Matriz Vulnerabilidade x Impacto
3. Cyber por Processo de Negócio
4. Efetividade de Controles Internos
5. Planos de Ação e Atrasos
6. Compliance e Obrigações (LGPD)
7. Incidentes e Continuidade (BIA)

A Visão da Alta Gestão (Página 1)

12

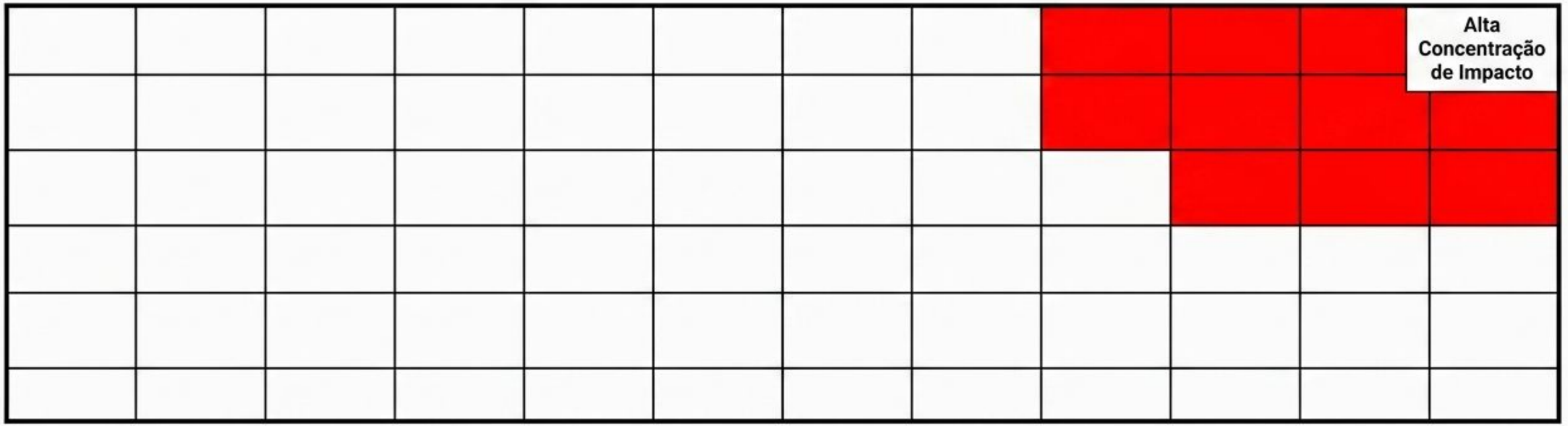
Processos Críticos Expostos

8

Controles Internos Ineficazes

5

Planos de Ação Críticos Vencidos



O Papel Fundamental do GRC

Segurança: Vincula vulnerabilidades à matriz corporativa.

Riscos & Compliance: Controla obrigações e avaliações contínuas.

Governança: Transforma dados técnicos em report executivo para decisão.

Sistema de GRC: Centralização, Rastreabilidade e Trilha de Auditoria.

Ações Estratégicas Imediatas

1. Criar uma taxonomia de riscos cyber integrada à matriz corporativa.
2. Mapear ativos digitais críticos aos processos de negócio.
3. Vincular Controles Internos aos riscos e testar sua efetividade real.
4. Definer o apetite de risco e critérios claros de escalonamento executivo.
5. Estabelecer Monitoramento Contínuo integrado à resposta a incidentes e BIA.

O Valor Entregue à Organização

Segurança da Informação

Orçamento e Prioridade. Sai da defesa técnica isolada e ganha justificativa de negócio para investimentos.

Riscos & Compliance

Visão Unificada. Conecta ameaças invisíveis às normativas (ex: LGPD) e à matriz operacional.

Auditoria Interna

Rastreabilidade Total. Evidências claras, testes de Controles Internos auditáveis e fim das caixas-pretas de TI.

Comitê Executivo / Conselho

Decisão Clara. Substitui relatórios de volume de ataques por métricas de de exposição financeira e operacional.

O Checklist Prático de Maturidade

- [x] O tema ‘Cyber’ possui dono claro e está na matriz corporativa de riscos?
- [x] Vulnerabilidades de TI estão mapeadas aos processos de negócio?
- [ ] Os Controles Internos de segurança passam por Monitoramento Contínuo e testes?
- [ ] Planos de ação atrasados geram escalonamento automático para a diretoria?
- [ ] O Conselho recebe relatórios de impacto ao invés de volume de CVEs?

“Risco cibernético não é isolado. É corporativo. E só vira decisão quando vulnerabilidade, ativo, processo, controle, compliance auditoria passam a falar a mesma língua.”

Avalie sua maturidade e inicie a integração.

Uma parceria risklab. + Perinity risklab.

perinity