csurface

GUIA · CYBER RISK QUANTIFICATION

Guia de implementação de Quantificação de Risco Cibernético

O passo a passo completo para transformar a incerteza do risco cibernético em exposição financeira mensurável — da preparação inicial à metodologia FAIR, aos oito estágios de implementação e ao relatório que o conselho aprova.

TEMA	PÚBLICO	EDIÇÃO
Quantificação de Risco	**CISO · Risco · CFO · Comitê de Auditoria**	**2026**

LEITURA	CLASSIFICAÇÃO	FONTE
~21 páginas	**Público**	**Plataforma CSURFACE**

INTRODUÇÃO

Quantificar o risco é uma decisão de gestão

O que é o CRQ, para quem este guia foi escrito e o caminho que ele percorre da preparação ao relatório.

CUSTO MÉDIO DE VIOLAÇÃO

R$ 7,19 mi

média no Brasil em 2025 (IBM Cost of a Data Breach) [4]

SANÇÃO ADMINISTRATIVA LGPD

2%

do faturamento por infração, limitada a R$ 50 milhões

ESTÁGIOS DE IMPLEMENTAÇÃO

8

do escopo à iteração contínua, detalhados neste guia

Cyber Risk Quantification (CRQ) é a disciplina de medir o risco cibernético em termos financeiros — em reais, e não em rótulos de cor. Em vez de afirmar que "o risco é alto", o CRQ responde a uma pergunta que o conselho sabe gerir: **quanto a organização deve perder, por ano, em decorrência de incidentes cibernéticos**, e qual o pior caso razoável dessa perda.

A resposta vem na forma de duas grandezas: a **perda anual esperada (ALE)** e o **Value at Risk (VaR)**, geralmente reportado nos percentis P90 e P99. São as mesmas grandezas com que a tesouraria, a área de seguros e a auditoria já trabalham para outros riscos corporativos. O CRQ apenas traz o risco cibernético para esse mesmo plano.

Este é o **guia completo de implementação**. O whitepaper de CRQ apresenta a tese em síntese; este documento é o aprofundamento prático — destinado a quem precisa montar e sustentar o programa.

Para quem é este guia. Para o **CISO** que precisa defender o orçamento; para a área de **Risco** que integra o cibernético ao mapa corporativo; para o **CFO** que dimensiona reservas e seguro; e para o **comitê de auditoria** que precisa de uma trilha defensável diante do regulador.

O que este guia cobre

- Os **obstáculos** a vencer antes de iniciar o programa.
- Por que a **matriz qualitativa 5×5** falha como instrumento de decisão.
- A metodologia **FAIR** e sua decomposição do risco.
- Os **oito estágios** de implementação, detalhados um a um.
- Boas práticas, armadilhas e um **exemplo trabalhado** reproduzível na calculadora pública.

PARTE 01 · PREPARAÇÃO

Os obstáculos a vencer antes de começar

Sete pré-condições que determinam se o programa de CRQ entrega valor ou se trava no caminho.

Um programa de quantificação não fracassa por falta de fórmula — fracassa por falta de preparo. Antes de modelar a primeira variável, vale verificar se as sete condições abaixo estão minimamente satisfeitas. Nenhuma precisa estar perfeita; todas precisam estar endereçadas.

As sete pré-condições

1. **Inventário de ativos confiável.** Não se quantifica o que não se conhece. Um inventário incompleto produz uma exposição subestimada — e uma falsa sensação de controle.
2. **Dados e telemetria mapeados.** Identificar as fontes é prioridade: custo de incidentes passados, tempo de indisponibilidade, multas regulatórias e *breach intelligence* de mercado. Saber quais dados são relevantes vem antes de coletá-los.
3. **Linguagem comum.** Segurança opera em CVE e CVSS; o conselho delibera em reais e EBITDA. Sem essa tradução formal, o programa não obtém adesão da liderança e perde patrocínio antes de produzir resultado.
4. **Calibração de estimativas.** Na ausência de dados históricos, recorra a estimativas de especialistas estruturadas como intervalos de confiança — não como valores pontuais sem incerteza. Um intervalo bem calibrado reflete a realidade do risco com mais fidelidade do que um número exato desprovido de embasamento.
5. **Apetite de risco em termos financeiros.** Quanto de exposição anual, em reais, o conselho tolera? Sem esse limite definido, não há referência contra a qual comparar o resultado do modelo.
6. **Evitar os dois erros opostos.** De um lado, a falsa precisão — um número exato apresentado sem intervalo de incerteza. Do outro, a paralisia de aguardar a implementação do "FAIR completo" (12 meses ou mais) antes de entregar qualquer resultado. A abordagem correta é iniciar com escopo restrito e rigor metodológico, expandindo gradualmente à medida que o programa demonstra valor.
7. **Equipe multifuncional.** CRQ não é um programa exclusivo da área de segurança. A sua execução requer a participação de risco, segurança, finanças e unidades de negócio — cada função contribui com uma parcela insubstituível dos dados e do julgamento especializado.

O erro de partida mais comum. Tratar a quantificação como um exercício técnico isolado da área de segurança. Sem finanças à mesa, faltam os dados de custo; sem risco corporativo, o resultado não chega ao mapa de riscos; sem patrocínio do conselho, o programa não sobrevive ao primeiro trimestre. A composição da equipe é decisão estratégica, não detalhe operacional.

Princípio orientador. Maturidade em CRQ é um processo de avanço incremental. Iniciar com escopo restrito, endereçando parcialmente as sete pré-condições, produz resultados mais cedo e com maior aderência à realidade operacional do que aguardar condições ideais que raramente se concretizam.

PARTE 02 · O PROBLEMA DO QUALITATIVO

Por que a matriz 5×5 falha como dado

Três falhas estruturais da matriz de risco vermelho-amarelo-verde — com exemplos concretos.

A matriz de risco 5×5 é popular pela simplicidade. Mas a pesquisa acadêmica sobre o instrumento — em especial o trabalho de Anthony (Tony) Cox[2] e a crítica de Douglas Hubbard[3] aos *heat maps* — mostra que essa simplicidade esconde defeitos que comprometem a decisão. Esta página trata das três primeiras falhas; a próxima conclui a crítica.

Falha 1 — Resolução pobre e compressão de faixa

Uma matriz 5×5 tem apenas **25 células** para representar um universo contínuo e ilimitado de risco. Riscos quantitativamente muito diferentes são alocados na mesma célula. A pesquisa de Tony Cox mostra que matrizes típicas comparam corretamente **menos de 10% dos pares de riscos**.

> **Exemplo.** Um risco de exposição de aproximadamente **R$ 200 mil/ano** e outro de cerca de **R$ 8 milhões/ano** podem ambos ser rotulados "Alto" na mesma célula. Para o conselho, são o mesmo risco — e o capital de remediação é alocado de forma equivocada, sem que o desvio seja percebido.

Falha 2 — Inversão de risco e reversão de ranking

Quando probabilidade e impacto são **negativamente correlacionados**, a matriz pode atribuir a categoria **maior** ao risco quantitativamente **menor**. Cox conclui que, nesses casos, a matriz é "pior que inútil" — ela inverte ativamente a prioridade correta.

> **Exemplo.** Compare um evento raro de impacto altíssimo (uma fraude catastrófica improvável) com um evento frequente de impacto moderado. Conforme as bordas das faixas, a matriz pode classificar o segundo como mais grave que o primeiro — quando o primeiro tem perda anual esperada maior.

Falha 3 — Subjetividade e inconsistência

"Probabilidade alta" significa 30%? 70%? Sem escalas numéricas definidas, cada avaliador interpreta os rótulos de maneira distinta. O **mesmo risco recebe células diferentes** conforme quem preenche a matriz.

O resultado é que a matriz não registra dado — registra opinião. E opinião não é auditável, não é comparável entre áreas e não sobrevive à rotatividade de quem a produziu.

> **Exemplo.** Dois analistas avaliam o mesmo risco de indisponibilidade. Um, conservador, marca "Probabilidade média"; o outro, recém-saído de um incidente parecido, marca "Alta". A matriz move o risco de uma cor para outra — e nada na realidade do risco mudou.

> **O fio condutor.** As três falhas têm a mesma raiz: a matriz substitui a grandeza por um rótulo. Rótulos não têm aritmética, não têm escala e não têm unidade. Sem isso, não há como o instrumento sustentar uma decisão de capital.

PARTE 02 · O PROBLEMA DO QUALITATIVO (CONT.)

A matriz não agrega nem dialoga

As três falhas finais — e o que o conselho perde quando o risco chega apenas colorido.

Falha 4 — A matriz não agrega

Dois riscos "Altos" não somam para "Muito Alto" de forma coerente — não há aritmética por trás das cores. Não é possível somar a exposição de um **portfólio inteiro de riscos** dentro de uma matriz.

> **Exemplo.** O conselho pergunta: "Qual a nossa exposição cibernética total?" Com 30 riscos espalhados pela matriz, a única resposta possível é uma contagem de cores — "temos 8 vermelhos". O total financeiro, que é o que o conselho pediu, a matriz não fornece.

Falha 5 — Viés de centralização

Avaliadores tendem a evitar os extremos das escalas e a agrupar quase tudo nas células do meio. A matriz **perde poder de discriminação** justamente onde mais precisaria dele.

> **Exemplo.** Num inventário de 40 riscos, 32 são classificados como "Médio/Médio". A matriz que deveria priorizar passa a homogeneizar — e a área de segurança volta a decidir por instinto qual risco tratar primeiro.

Falha 6 — Não conversa com o apetite de risco

O conselho define tolerância em **reais**: "não aceitamos uma exposição anual acima de R$ X". O rótulo "Alto" não se compara a esse limite financeiro — está numa escala diferente, sem ponte entre as duas.

> **Exemplo.** O apetite aprovado é de R$ 5 milhões de exposição anual. A matriz aponta "3 riscos Altos". É impossível dizer se a organização está dentro ou fora do apetite — o instrumento e o limite não se falam.

Conclusão das seis falhas. A matriz qualitativa tem um uso legítimo: *triagem inicial* de riscos recém-identificados, quando ainda não há dado nenhum. O equívoco está em tratá-la como a resposta financeira que o conselho espera. Para decisão de capital, ela precisa dar lugar a um modelo quantitativo.

ATENÇÃO **A matriz comunica**
Prioridade relativa grosseira entre riscos já conhecidos — útil como ponto de partida.

CRÍTICO **A matriz não comunica**
Magnitude, agregação de portfólio, trade-off de capital nem comparação com o apetite de risco.

PARTE 03 · A METODOLOGIA

FAIR: decompor o risco para poder calculá-lo

O padrão aberto que transforma o risco opaco em variáveis observáveis e calculáveis.

A DECOMPOSIÇÃO DO FAIR · DO RISCO OPACO À VARIÁVEL CALCULÁVEL

1 **Risco**
Frequência de eventos de perda × Magnitude da perda — o todo, decomposto.

→

2 **Frequência**
Frequência de evento de ameaça × Vulnerabilidade — a chance anual de perda.

→

3 **Magnitude**
Perda primária + Perda secundária — o custo esperado por evento.

→

4 **Distribuição**
Cada variável torna-se uma faixa probabilística para a simulação.

→

5 **Monte Carlo**
Milhares de simulações geram ALE e VaR (P50 / P90 / P99).

O princípio: separar e quantificar

O **FAIR — Factor Analysis of Information Risk**[1] é um padrão aberto que decompõe o risco em variáveis observáveis, em vez de tratá-lo como um todo opaco. A equação central é simples:

Risco = Frequência de eventos de perda × Magnitude da perda
Frequência = Freq. de evento de ameaça × Vulnerabilidade
Magnitude = Perda primária + Perda secundária

A **frequência de evento de ameaça** é quantas vezes, por ano, um agente tenta atingir o ativo. A **vulnerabilidade** é a probabilidade de que a tentativa tenha sucesso. A **perda primária** é o custo direto do incidente; a **secundária** inclui multas, perda de clientes e dano de marca.

Distribuições, não pontos únicos

O diferencial do FAIR é que cada variável é estimada como uma **distribuição de probabilidade** — uma faixa com mínimo, máximo e valor mais provável — e não como um número exato. Isso reconhece a incerteza inerente ao risco, em vez de escondê-la.

Sobre essas distribuições opera a **simulação de Monte Carlo**: milhares de cenários amostrados a partir das faixas probabilísticas, cujo resultado agregado é uma curva de perda. Dessa curva se extraem o **ALE** (perda anual esperada, o valor médio) e o **VaR** nos percentis P50, P90 e P99 — o pior caso razoável.

O FAIR não substitui o julgamento técnico — ele o organiza. Cada estimativa fica explícita, documentada e revisável. Quando um número é questionado pela auditoria, é possível mostrar exatamente de qual variável e de qual faixa ele veio. É essa rastreabilidade que torna o resultado defensável.

PARTE 04 · IMPLEMENTAÇÃO

Os oito estágios do programa de CRQ

Visão geral do percurso — do escopo inicial à iteração contínua.

O PERCURSO DE IMPLEMENTAÇÃO · OITO ESTÁGIOS

1 **Escopo** — Definir as perguntas a responder.
→ 2 **Framework** — Escolher a metodologia — FAIR.
→ 3 **Inventário** — Mapear e valorar os ativos.
→ 4 **Dados** — Coletar telemetria e histórico.
5 **Modelar** — Decompor e estimar distribuições.
→ 6 **Simular** — Monte Carlo, ALE e VaR.
→ 7 **Comunicar** — Traduzir para a linguagem do board.
→ 8 **Iterar** — Recalibrar de forma contínua.

Quadro-resumo dos oito estágios

#	ESTÁGIO	ENTREGA PRINCIPAL
1	Escopo e objetivos	As perguntas que o relatório deve responder
2	Escolha do framework	FAIR adotado como base metodológica
3	Inventário e valoração	Lista de ativos com valor de negócio
4	Coleta de dados	Telemetria de ameaça, controles e histórico
5	Modelagem	Variáveis FAIR estimadas como distribuições
6	Simulação	ALE e VaR (P50 / P90 / P99)
7	Comunicação	Relatório financeiro para o board
8	Iteração	Recalibragem contínua do modelo

Não é um projeto linear de prazo fixo. Os oito estágios descrevem um ciclo iterativo. A primeira execução pode cobrir um único ativo crítico em poucas semanas; as iterações subsequentes ampliam o escopo e refinam as estimativas. O programa consolida maturidade a cada ciclo concluído — não em uma entrega única e definitiva.

Como ler as próximas páginas

Cada um dos **oito estágios** ocupa uma página dedicada — com o objetivo, o passo a passo executável, os insumos necessários e o erro comum a evitar. A simulação, pela sua densidade, ocupa duas páginas.

Um **caso trabalhado único** — a quantificação do risco de e-commerce de uma rede varejista — atravessa os oito estágios, com números reais em cada etapa, do escopo inicial ao relatório levado ao conselho.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 1 DE 8

Estágio 1 · Escopo e objetivos

Declarar a decisão que o número vai sustentar e recortar o primeiro cenário de risco a quantificar.

Objetivo do estágio. Concluir com três definições registradas: a **decisão-alvo** que o relatório deve sustentar, as **perguntas de negócio** a responder e um **cenário de risco único** — um par agente × ativo — escolhido para a primeira iteração.

Como executar — passo a passo

1. **Identifique a decisão.** A quantificação é, na prática, insumo de uma decisão. Aprovar um orçamento de remediação, dimensionar o seguro cibernético ou aceitar formalmente um risco são decisões distintas, e cada uma exige um recorte diferente. Nomeie a decisão antes de qualquer cálculo.
2. **Escreva as perguntas em linguagem de negócio.** "Qual a exposição anual, em reais, deste cenário?" "O investimento previsto reduz a exposição mais do que custa?" Perguntas formuladas em termos técnicos produzem relatórios técnicos — não decisões de gestão.
3. **Recorte um cenário de risco único.** Não se quantifica "o risco cibernético" como um todo. A unidade de análise do FAIR é o cenário: um **agente de ameaça** específico, agindo sobre um **ativo** específico, produzindo uma **forma de perda** específica.
4. **Fixe o horizonte e a unidade.** O padrão de mercado é uma janela de 12 meses, com resultado em reais. Toda variável estimada e todo número reportado passam a obedecer a esse recorte.
5. **Nomeie o patrocinador.** A decisão-alvo precisa de um responsável no nível adequado — CFO ou comitê de auditoria. Sem patrocínio executivo declarado, o resultado não se converte em deliberação.

No caso · a varejista

O exemplo trabalhado deste guia acompanha uma **rede varejista** — R$ 1,2 bilhão de faturamento anual, e-commerce próprio responsável por cerca de R$ 28 milhões de receita por mês.

Decisão-alvo: aprovar, ou não, um investimento de **R$ 1,2 milhão** em WAF gerenciado e hardening da aplicação de e-commerce.

CENÁRIO ESCOLHIDO PARA A 1ª ITERAÇÃO	
Agente de ameaça	Atacante externo
Ativo	Aplicação de e-commerce
Forma de perda	Exfiltração de dados de clientes
Horizonte · unidade	12 meses · R$

Erro comum. Iniciar pela escolha de ferramentas e sistemas antes de definir a pergunta de negócio. Sem clareza sobre o que o relatório deve responder — e para quem —, o programa produz análises tecnicamente corretas que não fundamentam nenhuma decisão de gestão.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 2 DE 8

Estágio 2 · Escolher o framework

Adotar uma metodologia padronizada, a ferramenta de simulação e o padrão de documentação.

Objetivo do estágio. Adotar o **FAIR** como taxonomia, escolher a **ferramenta de simulação** adequada ao estágio de maturidade do programa e fixar o **padrão de documentação** que tornará cada estimativa auditável.

Como executar — passo a passo

1. **Adote o FAIR como taxonomia.** O *Factor Analysis of Information Risk* é um padrão aberto, mantido pelo FAIR Institute, compatível com ISO 27005 e COSO ERM. Adotá-lo dá ao programa um vocabulário comum e uma decomposição já consolidada.
2. **Liste as variáveis que o modelo exige.** O FAIR decompõe o risco em cinco variáveis a estimar: Frequência de Evento de Ameaça, Vulnerabilidade, Perda Primária, Frequência de Perda Secundária e Perda Secundária. São elas que os estágios seguintes vão alimentar.
3. **Escolha a ferramenta de simulação.** Para a primeira iteração, uma planilha com função de Monte Carlo é suficiente. À medida que o escopo cresce, ferramentas dedicadas — FAIR-U, bibliotecas open-source ou um módulo de CRQ — ganham eficiência e reduzem o erro operacional.
4. **Defina o padrão de documentação.** Cada estimativa registra fonte, faixa, autor e data — uma *ficha de variável*. É essa trilha que permite, diante de um questionamento da auditoria, mostrar de qual dado e de qual faixa um número derivou.
5. **Concilie com o que já existe.** Mapeie o FAIR ao ISO 27005 e ao COSO ERM já adotados, para que o resultado entre no mapa de riscos corporativo sem retrabalho nem terminologia concorrente.

Por que um padrão aberto

Um framework padronizado e documentado é o que torna o resultado **reproduzível** — outra pessoa, com os mesmos dados, chega ao mesmo número — e **comparável** ao longo do tempo. Um método próprio e não documentado não oferece nenhuma das duas garantias.

No caso · a varejista

A varejista adota o **FAIR**. Para o primeiro ciclo, a ferramenta é uma **planilha de Monte Carlo** de 100.000 iterações. A documentação segue o modelo de uma ficha por variável, e o resultado será espelhado no mapa de riscos corporativo já mantido sob ISO 27005.

Erro comum. A adoção de um método próprio e não documentado. Tal abordagem compromete a auditabilidade e a reprodutibilidade dos resultados, impede a comparação consistente ao longo do tempo e não se sustenta no longo prazo, pela falta de aderência a normas e padrões de mercado.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 3 DE 8

Estágio 3 · Inventário e valoração

Listar os ativos que compõem o cenário e atribuir a cada um o seu valor de negócio.

Objetivo do estágio. Produzir a lista completa dos ativos que sustentam o cenário, cada um com um **valor de negócio** — quanto a organização perde se aquele ativo for comprometido, não o seu valor contábil.

Como executar — passo a passo

1. **Liste os ativos que compõem o cenário.** Não apenas a aplicação visível: tudo o que a sustenta — servidores, bancos de dados, APIs, integrações e componentes de terceiros embutidos no código.
2. **Registre o que cada ativo sustenta.** A receita que ele viabiliza, os dados que processa, a função operacional que desempenha. Esse registro é a base da valoração.
3. **Valore pela perda.** O valor de negócio corresponde à perda decorrente do comprometimento do ativo: receita interrompida por dia de indisponibilidade, número de registros de dados pessoais expostos, custo de reconstrução. O valor contábil é uma referência diferente, imprópria para essa finalidade.
4. **Marque a dependência externa.** Componentes de terceiros integrados ao ativo entram no inventário — são superfície cuja responsabilidade recai sobre a organização, independentemente da autoria do código.
5. **Verifique a completude.** O ativo ausente do inventário é o que subestima toda a exposição. Um inventário derivado de descoberta contínua da superfície externa reduz esse ponto cego de forma estrutural.

No caso · a varejista

Os ativos que compõem o cenário de e-commerce e o valor de negócio de cada um:

ATIVO	SUSTENTA	VALOR DE NEGÓCIO
Aplicação de e-commerce	Canal de venda online	R$ 28 mi receita/mês
Base de dados de clientes	Cadastro e histórico	2,3 mi de registros PII
Gateway de pagamento	Transações com cartão	Escopo PCI-DSS
3 APIs públicas	App mobile e parceiros	Superfície de entrada

Erro comum. A adoção de um inventário incompleto como base de cálculo. Ativos expostos ausentes do levantamento produzem exposição sistematicamente subestimada — comprometendo a validade do modelo e a credibilidade do relatório perante a auditoria.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 4 DE 8

Estágio 4 · Coletar dados e telemetria

Reunir os insumos que vão calibrar cada uma das cinco variáveis do modelo FAIR.

Objetivo do estágio. Para cada variável do FAIR, identificar e reunir a fonte de dado que a calibra — priorizando o dado interno e completando, onde ele falta, com referências de mercado e estimativas calibradas.

Como executar — passo a passo

1. **Mapeie a fonte de cada variável antes de coletar.** Saber qual dado calibra qual variável evita uma coleta dispersa, que reúne muito dado sem alimentar o modelo.
2. **Reúna o dado de frequência.** Frequência de Evento de Ameaça e Vulnerabilidade vêm de logs de WAF e IDS, inteligência de ameaças, resultados de testes de intrusão, da postura de patch e da exploitabilidade conhecida das falhas expostas.
3. **Reúna o dado de magnitude.** Perda Primária e Secundária vêm do custo de incidentes passados, de contratos de resposta a incidente, do histórico setorial de sanções LGPD e de referências de mercado.
4. **Priorize o dado interno.** O dado próprio — um incidente já ocorrido, um custo já apurado — é o mais valioso. Esgote-o antes de recorrer a referências externas.
5. **Onde faltar dado, calibre a estimativa.** A ausência de histórico não interrompe o programa: registre uma faixa de especialista calibrada, e não um número exato sem embasamento.

Onde cada variável é calibrada

VARIÁVEL FAIR	FONTE DE DADO	INSUMO DA CSURFACE
Freq. Evento de Ameaça	Logs WAF/IDS · threat intel	Threat sensor — atividade real de ameaça
Vulnerabilidade	Pentest · postura de patch	Inteligência de exploits · exploitabilidade
Perda Primária	Incidentes passados · contratos IR	—
Perda Secundária	Histórico LGPD · churn · IBM 2025	—

O threat sensor e a inteligência de exploits da CSURFACE alimentam diretamente os dois insumos mais difíceis de estimar — a frequência de ameaça e a vulnerabilidade. Detalhe na página 17.

Calibração — o que é. Calibrar uma estimativa é treinar o especialista a fornecer um intervalo dentro do qual o valor real cai com 90% de confiança. É uma habilidade treinável: um especialista calibrado produz faixas confiáveis mesmo na ausência de dado histórico.

Erro comum. Condicionar o avanço do programa à disponibilidade de dados completos. A ausência de dados históricos internos não impede a modelagem — impede apenas a modelagem sem calibração.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 5 DE 8

Estágio 5 · Modelar as distribuições

Converter cada variável do FAIR em uma distribuição de probabilidade de três pontos.

Objetivo do estágio. Transformar cada uma das cinco variáveis em uma **distribuição** — mínimo, valor mais provável e máximo —, registrando a fonte de cada ponto. É o conjunto dessas distribuições que a simulação irá processar.

Por que uma distribuição, não um número

Um valor único descarta a incerteza — e a incerteza *é* o dado mais importante do risco. Uma distribuição de três pontos declara, de forma explícita, o que se sabe e o que não se sabe sobre cada variável.

A maioria das variáveis do FAIR é modelada como uma distribuição **PERT (BetaPERT)**: uma curva suave, ancorada no valor mais provável e limitada pelo mínimo e pelo máximo. Sua média é **(mín + 4 × mais provável + máx) ÷ 6**.

Como executar — passo a passo

1. **Defina o intervalo de 90%.** O mínimo e o máximo que cercam 90% da probabilidade — não o pior caso absoluto imaginável.
2. **Acrescente o valor mais provável.** O ponto em que a estimativa se concentra, entre o mínimo e o máximo.
3. **Escolha a forma.** PERT para a maioria das variáveis; uma forma de cauda mais longa, como a lognormal, para magnitudes de perda com cauda pesada.
4. **Submeta à revisão multifuncional.** Risco, segurança e finanças validam as faixas antes de a simulação ser executada.

No caso · as cinco distribuições da varejista

VARIÁVEL	MÍN	PROVÁVEL	MÁX
Freq. Evento de Ameaça	2	**5**	14 /ano
Vulnerabilidade	3%	**8%**	20%
Perda Primária	0,9	**2,4**	6,0 mi
Freq. Perda Secundária	70%	**90%**	100%
Perda Secundária	1,5	**6,0**	22,0 mi

Freq. de Evento de Ameaça em tentativas qualificadas por ano. Perdas em R$ milhões. Fontes: logs de WAF, teste de intrusão, incidente interno de 2023 e IBM Cost of a Data Breach 2025.

Erro comum. Substituir distribuições por valores pontuais. Essa simplificação elimina a representação explícita da incerteza — característica que confere ao modelo tanto a sua honestidade técnica quanto a sua defensabilidade perante o comitê de auditoria.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 6 DE 8 · PARTE 1

Estágio 6 · Simular — o método de Monte Carlo

O que a simulação faz, por que ela é necessária e como o seu algoritmo opera.

O que é a simulação de Monte Carlo

Monte Carlo é uma técnica que **executa o modelo milhares de vezes**. Em cada execução, sorteia um valor de cada distribuição de entrada e calcula a perda daquela execução. O conjunto de todos os resultados forma a **curva de perda anual** — a distribuição completa dos resultados possíveis.

Por que ela é necessária

Não é possível somar e multiplicar cinco distribuições de probabilidade analiticamente, à mão. Um cálculo de ponto único — multiplicar apenas os valores médios — **descarta a incerteza** e devolve um número que esconde a faixa de resultados. A simulação propaga a incerteza de cada entrada até o resultado final.

O ALGORITMO · UM "ANO POSSÍVEL" POR ITERAÇÃO

1 Sorteie frequência
Sorteie a Freq. de Evento de Ameaça e a Vulnerabilidade. O produto é λ — eventos de perda esperados no ano.

→

2 Conte os eventos
Uma distribuição de Poisson com média λ converte a frequência esperada em uma contagem inteira: 0, 1, 2…

→

3 Componha a perda
Para cada evento, sorteie a Perda Primária; pela Freq. de Perda Secundária, decida se há perda secundária e sorteie-a.

4 Some o ano
A soma das perdas dos eventos é a perda total daquele ano simulado.

→

5 Repita
De 10.000 a 100.000 vezes. Cada repetição é um ano possível, independente dos demais.

→

6 Agregue
A média das perdas anuais é o ALE; os percentis da curva são o VaR.

Quantas iterações. Dez mil iterações bastam para uma leitura estável da média (ALE). Para que a cauda — o VaR P99 — fique precisa, recomenda-se 100.000. No exemplo da varejista, a simulação rodou **100.000 iterações** sobre as cinco distribuições do estágio 5.

Uma iteração ilustrada — um ano possível

Para tornar o algoritmo concreto, acompanhe uma única iteração da simulação da varejista:

1 · Sorteio de frequência	Ameaça 6,1 × Vuln. 10,5% → λ = 0,64
2 · Contagem · Poisson (λ = 0,64)	1 evento neste ano
3 · Perda do evento	Primária R$ 2,1 mi + Secundária R$ 7,4 mi
4 · Perda do ano	R$ 9,5 mi

Esta iteração contribui com **R$ 9,5 milhões**. A iteração seguinte, com um λ menor, pode sortear **zero evento** e contribuir com R$ 0. A média de 100.000 iterações como esta é o ALE; o ordenamento de todas elas, da menor para a maior, produz a curva de perda da próxima página.

Por que uma distribuição de Poisson

A frequência λ é uma **média** — mas o número de incidentes em um ano concreto é um inteiro: 0, 1, 2. A distribuição de Poisson é o instrumento estatístico que converte uma taxa média de eventos independentes na probabilidade de cada contagem possível.

Com o λ médio de **0,55** do cenário da varejista, a Poisson atribui cerca de **58%** de probabilidade a nenhum evento no ano, **32%** a exatamente um e **10%** a dois ou mais. É essa assimetria — a maioria dos anos sem perda, alguns poucos com perda elevada — que molda o resultado do estágio.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 6 DE 8 · PARTE 2

Estágio 6 · Simular — ALE e VaR do caso

Ler o resultado da simulação: a perda média, a cauda e a curva de excedência.

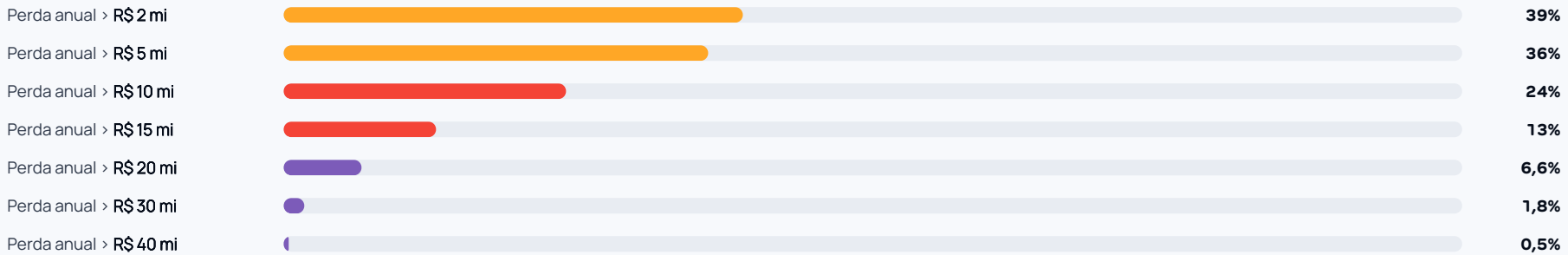
ALE · PERDA ANUAL ESPERADA
R$ 5,3 mi
a média da curva de perda

VAR · PERCENTIL 90
R$ 16,8 mi
o número para decisão de capital

VAR · PERCENTIL 99
R$ 34,4 mi
o pior caso razoável

Curva de excedência · a varejista

A probabilidade de a perda anual do cenário de e-commerce superar cada patamar — a tradução da incerteza em números de decisão:



Como ler o resultado

ALE — R$ 5,3 mi. A perda média anual do cenário. É o valor para o orçamento recorrente de risco e o ponto de comparação com o apetite aprovado pelo conselho.

VaR P90 — R$ 16,8 mi. Em 1 de cada 10 anos, a perda supera esse valor. É a referência para decisões de capital e para a priorização de remediações.

VaR P99 — R$ 34,4 mi. O pior caso razoável. Base para o dimensionamento de reservas de contingência e da cobertura de seguro cibernético.

PERCENTIL DA CURVA	PERDA ANUAL	LEITURA
P50 · mediana	R$ 0	maioria dos anos sem perda
P75	R$ 9,7 mi	1 ano em 4 supera este valor
P90	R$ 16,8 mi	decisão de capital
P99	R$ 34,4 mi	reservas e seguro

A leitura que mais surpreende o conselho. Em cerca de **60% dos anos simulados, a perda foi R$ 0** — o incidente não ocorre. A mediana (P50) do cenário é, portanto, zero. O ALE de R$ 5,3 milhões é uma média que incorpora os anos em que o incidente de fato ocorre. É exatamente por isso que o relatório reporta a média e a cauda — nunca a mediana isolada, que sugeriria, falsamente, ausência de risco.

Erro comum. Reportar exclusivamente a média (ALE) e omitir a análise de cauda. O VaR P99 — o pior caso razoável — é a métrica que fundamenta o dimensionamento de reservas e a contratação de seguro cibernético; sem ele, o relatório é incompleto para uma decisão de capital.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 7 DE 8

Estágio 7 · Comunicar ao conselho

Traduzir a curva de perda em uma recomendação: o número, o apetite e o trade-off da decisão.

Objetivo do estágio. Converter o resultado da simulação em um relatório de uma página que o conselho possa deliberar — abrindo pelo número, comparando-o ao apetite de risco e expondo o trade-off de cada alternativa de remediação.

Como executar — passo a passo

1. **Abra com o número, não com o método.** "A exposição anual deste cenário é de R$ 5,3 milhões; o pior caso razoável é de R$ 34,4 milhões." A metodologia vai para o apêndice.
2. **Compare ao apetite de risco.** Posicione a exposição contra o limite, em reais, que o conselho aprovou. É essa comparação que indica se há ou não decisão a tomar.
3. **Apresente o trade-off.** Quanto cada alternativa de remediação custa e quanto reduz o ALE. É o que transforma um número em uma recomendação acionável.
4. **Mostre a faixa inteira.** O relatório expõe a incerteza — a curva de perda —, evitando a falsa precisão de um valor isolado.
5. **Anexe a trilha.** As fichas de variável e as premissas vão em apêndice, à disposição da auditoria, fora do corpo principal do relatório.

No caso · a recomendação ao conselho

O investimento de **R$ 1,2 milhão** em WAF gerenciado e hardening reduz a Vulnerabilidade do valor mais provável de 8% para 3%. O modelo, recalculado, devolve:

MÉTRICA	HOJE	APÓS O INVESTIMENTO
ALE	R$ 5,3 mi	R$ 2,0 mi
VaR P90	R$ 16,8 mi	R$ 9,8 mi
VaR P99	R$ 34,4 mi	R$ 21,4 mi

A frase para o conselho. "O investimento de R$ 1,2 milhão reduz a exposição anual em R$ 3,3 milhões — de R$ 5,3 mi para R$ 2,0 mi — e o pior caso razoável em R$ 13 milhões. O retorno se dá já no primeiro ano. Recomendação: aprovar." Uma remediação se justifica quando reduz o ALE por mais do que custa.

Erro comum. Apresentar a metodologia e os parâmetros do modelo em lugar do resultado e da recomendação. O conselho necessita da exposição em reais e da análise de custo-benefício — não da descrição do processo que os produziu.

PARTE 04 · IMPLEMENTAÇÃO · ESTÁGIO 8 DE 8

Estágio 8 · Iterar e recalibrar

Manter o número válido conforme a realidade muda — e ampliar o escopo a cada ciclo.

Objetivo do estágio. Estabelecer o ciclo de recálculo que mantém o ALE aderente ao risco vigente — confrontando o previsto com o ocorrido, reapertando as distribuições e ampliando o escopo para o próximo cenário.

Como executar — passo a passo

1. **Defina os gatilhos de recálculo.** Uma mudança material no inventário, uma nova ameaça relevante, um controle implantado ou o encerramento de um trimestre disparam a revisão do modelo.
2. **Confronte o previsto com o ocorrido.** Houve evento no período? O custo apurado caiu dentro da faixa estimada? Esse confronto é o backtesting que valida — ou corrige — o modelo.
3. **Reaperte as distribuições.** Cada novo dado estreita uma faixa antes ampla. O modelo ganha precisão a cada ciclo concluído.
4. **Amplie o escopo.** Com o primeiro cenário consolidado, o próximo entra na fila. A soma dos cenários quantificados forma a exposição cibernética de portfólio.
5. **Versione cada relatório.** Data, premissas e resultado de cada ciclo ficam registrados — a trilha que demonstra a evolução do risco ao longo do tempo.

No caso · a varejista

Implantado o WAF gerenciado, a varejista define o **recálculo trimestral** do cenário de e-commerce. No primeiro trimestre após a remediação, a Vulnerabilidade observada nos logs confirma a queda projetada, e o ALE recai para a faixa prevista de **R$ 2,0 milhões**.

O confronto entre o previsto e o ocorrido — nenhum evento de perda no período, custos dentro da faixa estimada — valida o modelo. As distribuições são reapertadas com os novos dados, e a faixa de cada variável estreita.

Com o primeiro cenário consolidado, o **próximo entra no escopo**: o comprometimento do ERP por ransomware. Ele percorre os mesmos oito estágios. A soma dos cenários quantificados passa a formar a **exposição cibernética de portfólio** — o número que o conselho compara ao apetite de risco corporativo.

Por que o número precisa ser vivo. Um ALE calculado há 12 meses descreve um estado anterior do inventário, das ameaças e dos controles — não o perfil de risco vigente. A recalibragem periódica não é um refinamento opcional: é a condição que mantém o número válido como base de decisão.

Erro comum. Tratar o primeiro relatório como referência permanente. O inventário se expande, novas vulnerabilidades surgem e controles são implantados — a recalibragem periódica é condição de validade do número.

O ciclo se fecha — e recomeça. Concluído o oitavo estágio, o programa não termina: recomeça. Os oito estágios formam um ciclo, e cada volta amplia o escopo, estreita as distribuições e melhora a precisão do número. As próximas páginas reúnem as boas práticas e as armadilhas que distinguem um ciclo que sustenta decisões de um que produz números frágeis.

PARTE 05 · EXECUÇÃO

Boas práticas e armadilhas a evitar

O que separa um programa de CRQ que sustenta decisões de um que produz números frágeis.

Boas práticas

1. **Comece pequeno.** Quantifique primeiro um único ativo ou risco crítico. Um resultado de escopo restrito, metodologicamente consistente e defensável, tem mais valor institucional do que um plano abrangente que não se concretiza.
2. **Priorize os dados já disponíveis.** Telemetria de segurança, registros de incidentes, dados financeiros e referências de mercado já estão acessíveis — esgote essas fontes antes de estruturar coletas adicionais.
3. **Comunique sempre em reais.** O resultado obtém adesão da liderança quando apresentado na grandeza com que ela toma decisões. CVE e CVSS devem ser traduzidos em exposição financeira — sem exceção.
4. **Monitore e refine.** Revise as estimativas conforme novos dados chegam. O modelo ganha precisão a cada ciclo — desde que seja sistematicamente revisitado.
5. **Mantenha a equipe multifuncional.** Risco, segurança, finanças e unidades de negócio reunidos — condição necessária para que o número seja completo e para que a recomendação seja aceita pelas partes que precisam agir sobre ela.

Armadilhas a evitar

CRÍTICO **Falsa precisão**

Apresentar um número exato — "a exposição é R$ 11.137.482" — sem a faixa de incerteza. Um intervalo honesto é mais confiável que um ponto preciso e falso.

CRÍTICO **O "big bang" de 12 meses**

Tentar implementar o FAIR completo, em todo o escopo, antes de entregar qualquer valor. O programa perde patrocínio muito antes do primeiro resultado.

ATENÇÃO **Dados ruins, falsa segurança**

Alimentar o modelo com inventário incompleto ou estimativas não calibradas. O resultado parece sólido, mas descreve uma realidade que não existe.

O equilíbrio. A eficácia do CRQ reside entre dois extremos simétricos: a falsa precisão de um número exato sem intervalo de incerteza e a paralisia decorrente de aguardar um programa sem lacunas antes de produzir qualquer resultado. Um intervalo bem calibrado, entregue sobre escopo restrito e refinado a cada ciclo, é a trajetória que confere credibilidade duradoura ao programa.

PARTE 06 · A ABORDAGEM CSURFACE

Como a CSURFACE alimenta o framework

A plataforma supre os dois insumos mais difíceis do FAIR: o inventário e a frequência de ameaça.

O GARGALO DO FAIR

Dados de entrada

- Inventário desatualizado
- Frequência de ameaça estimada sem calibração
- Recalibragem anual

→

O QUE A CSURFACE FORNECE AO MODELO

Insumos vivos e contínuos

- Inventário da descoberta contínua
- Frequência calibrada pelo threat sensor
- Atividade real de ameaças
- Inteligência de exploits
- Indicadores de campanha
- Recalibragem contínua

O inventário vem da descoberta contínua

O estágio 3 — inventário e valoração — é, na prática, onde a maioria dos programas tropeça: não se quantifica o que não se conhece. A CSURFACE resolve esse gargalo na origem. A **descoberta contínua da superfície externa** mantém o inventário de ativos atualizado de forma permanente, com Machine Learning para classificação e atribuição de criticidade.

Isso significa que o modelo de CRQ não parte de uma planilha estática que envelhece — parte de um **inventário vivo**. Cada ativo novo descoberto entra automaticamente no escopo do cálculo.

A frequência de ameaça vem do threat sensor

A variável mais difícil de estimar no FAIR é a **frequência de evento de ameaça**. A CSURFACE a calibra com o **threat sensor**, que observa **atividade real de ameaças**: tentativas de exploração, inteligência de exploits, indicadores de campanha, parâmetros, métricas e integrações.

Essa calibragem vai **muito além** de CVSS, dos índices de probabilidade de exploração e dos catálogos de exploração ativa — esses scores são insumos entre vários, e não a base do modelo. O que pesa é o sinal ao vivo de ameaça observada contra ativos como os da organização.

A calculadora pública e o módulo integrado. A calculadora pública de risco é a porta de entrada: uma primeira leitura de exposição com poucos parâmetros. O **módulo CRQ integrado** substitui as estimativas setoriais pelo inventário real e mantém o **loop fechado** — o ALE se recalcula a cada mudança no inventário, na ameaça e na remediação.

PARTE 07 · APLICAÇÃO PRÁTICA

Simule você mesmo — um exemplo trabalhado

Reproduza este cálculo na calculadora pública: csurface.io/calculadora-de-risco.html

PERDA ANUAL ESPERADA (ALE)

R$ 11,1 mi

probabilidade ajustada × SLE

VALUE AT RISK · P90

R$ 20,5 mi

o número para decisão de capital

EXPOSIÇÃO A MULTA LGPD

R$ 17,5 mi

sanção potencial ponderada pela probabilidade

Passo a passo na calculadora

O cenário: uma **varejista**, faturamento de **R$ 1,2 bilhão**, 4.500 colaboradores, 8.700 ativos e maturidade de segurança intermediária — a mesma organização do caso trabalhado nos estágios deste guia. A calculadora estima a exposição **agregada** da organização; os estágios decompõem, pela metodologia FAIR, um **cenário específico** dentro dessa exposição. Acesse **csurface.io/calculadora-de-risco.html** e insira os parâmetros abaixo:

1. **Setor** — selecione *Varejo*. Define a probabilidade-base e o multiplicador de custo do setor.
2. **Faturamento anual** — informe *R$ 1,2 bilhão*. Entra no cálculo do SLE e no teto da multa LGPD.
3. **Número de colaboradores** — informe *4.500*. Serve como parâmetro de dimensionamento do porte da organização.
4. **Número de ativos** — informe *8.700*. Ajusta o SLE pelo tamanho da superfície de ataque.
5. **Maturidade de segurança** — selecione *Intermediária*. Modula a probabilidade ajustada.

A calculadora aplica o modelo recalibrado da CSURFACE e retorna ALE, VaR e exposição regulatória em segundos, sem cadastro.

O resultado retornado

MÉTRICA	VALOR	PARA QUE SERVE
Probabilidade ajustada	≈ 56%	Chance anual de incidente
SLE	R$ 19,8 mi	Perda por evento
ALE	R$ 11,1 mi	Orçamento anual
VaR P90	R$ 20,5 mi	Decisão de capital
VaR P99	R$ 39,9 mi	Reserva / seguro
Multa LGPD	R$ 17,5 mi	Exposição regulatória

A frase para o conselho. "Nossa exposição cibernética anual é de R$ 11,1 milhões, com VaR P90 de R$ 20,5 milhões e exposição regulatória de R$ 17,5 milhões." É esse enunciado — reproduzível na calculadora pública a partir dos parâmetros do exemplo — que converte uma apresentação técnica em uma deliberação de capital.

APÊNDICE

Metodologia e fontes

As referências que sustentam este guia e uma nota sobre a natureza das estimativas.

Referências

1. **FAIR Institute** — Factor Analysis of Information Risk. Padrão aberto de quantificação de risco em informação, base metodológica deste guia.
2. **Anthony (Tony) Cox** — "What's Wrong with Risk Matrices?", *Risk Analysis*, 2008. Análise das limitações estruturais das matrizes qualitativas de risco.
3. **Douglas Hubbard** — crítica a *heat maps* e aos métodos qualitativos de avaliação de risco, e defesa da medição quantitativa.
4. **IBM** — Cost of a Data Breach Report 2025. Custo médio de violação de dados no Brasil: R$ 7,19 milhões.

Nota metodológica

O caso trabalhado que atravessa este guia — a quantificação do cenário de e-commerce de uma rede varejista — foi obtido por **simulação de Monte Carlo** (100.000 iterações) sobre distribuições FAIR. O exemplo da página 19, na calculadora pública, aplica o modelo recalibrado da CSURFACE, que parte da média nacional do IBM Cost of a Data Breach 2025. Ambos descrevem um cenário **fictício e ilustrativo** — destinado a demonstrar o método, não a representar uma organização real.

O CRQ produz **distribuições de probabilidade**, não certezas. ALE e VaR são leituras de uma curva de perda simulada; a precisão do resultado depende diretamente da qualidade do inventário e dos dados de entrada — daí a ênfase deste guia na preparação e na iteração contínua.

Frameworks e regulações citados. FAIR, Monte Carlo, COSO ERM, ISO 27005, LGPD, BACEN e CVM são metodologias e regulações públicas, mencionadas como referência. Este é um material educacional; não substitui aconselhamento jurídico ou regulatório específico.

PRÓXIMOS PASSOS

Do guia à prática: comece com um número em reais

A Quantificação de Risco Cibernético é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Integrada em uma plataforma única, ela reúne descoberta contínua da superfície externa com Machine Learning, análise da cadeia digital de fornecedores, validação de exploitabilidade, inteligência de ameaças com priorização dinâmica, monitoramento de credenciais vazadas e quantificação financeira de risco. Opera de forma inteiramente externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM para aprofundamento do escopo.

Use a calculadora de risco

Reproduza o exemplo deste guia: estime o ALE e o VaR do seu setor em segundos, sem cadastro — a porta de entrada para a quantificação financeira.

Conheça o módulo CRQ

Em uma demonstração, veja a análise FAIR aplicada ao seu inventário real, com o loop fechado que mantém o ALE sempre atualizado.

Leia o whitepaper de CRQ

A versão síntese deste tema, com o modelo quantitativo da CSURFACE detalhado parâmetro por parâmetro.

Veja a sua exposição em reais — comece pela calculadora pública de risco

Abrir a calculadora de risco