csurface

WHITEPAPER · CYBER RISK QUANTIFICATION

Convertendo risco técnico em decisões financeiras

Cyber Risk Quantification: como a metodologia FAIR traduz vulnerabilidades, ativos e ameaças em perda anual esperada (ALE) e Value at Risk — em reais, na linguagem do comitê de auditoria.

CAPACIDADE	PÚBLICO	EDIÇÃO
Cyber Risk Quantification	**CISO · Risco · CFO · Auditoria**	**2026**

LEITURA	CLASSIFICAÇÃO	FONTE
10 páginas	**Público**	**Plataforma CSURFACE**

SUMÁRIO EXECUTIVO

Risco que não tem preço não tem decisão

A tese deste whitepaper, em uma página — o que o conselho precisa saber antes do detalhe metodológico.

CUSTO MÉDIO DE VIOLAÇÃO

R$ 7,19 mi

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

SANÇÃO ADMINISTRATIVA LGPD

2%

do faturamento por infração, limitada a R$ 50 milhões

TEMPO PARA IDENTIFICAR E CONTER

241 dias

média global em 2025 — o menor em nove anos (IBM)

Programas de segurança maduros produzem dados em abundância: número de CVEs abertas, tempo médio de remediação, cobertura de scans, postura de controles. São indicadores úteis para a gestão operacional do SOC. São, porém, praticamente **inúteis para o comitê de auditoria, para o conselho e para o CFO** — que precisam decidir orçamento, reservas de capital e apetite de risco.

A causa-raiz é uma falha de linguagem. A segurança opera em CVE, CVSS e MTTR; o conselho opera em exposição, EBITDA e retorno sobre o capital. Sem um denominador comum, o investimento em segurança é aprovado sem critério objetivo, a decisão de aceitar um risco não tem trade-off explícito e a renovação do seguro cibernético se apoia nas premissas de pior caso da corretora — não nas premissas da própria organização.

O **Cyber Risk Quantification (CRQ)** resolve essa lacuna. Aplicando a metodologia FAIR — Factor Analysis of Information Risk —, o CRQ converte a telemetria técnica em **exposição financeira mensurável**: perda anual esperada (ALE) e Value at Risk, expressos em reais. Esta é a métrica que o conselho aprova, que a auditoria externa documenta e que o regulador espera ver.

A tese. "Temos 47 vulnerabilidades críticas" é um dado sem unidade de decisão — não subsidia aprovação de orçamento, dimensionamento de reservas nem definição de apetite de risco. "Nossa exposição cibernética é de R$ 11 milhões ao ano, com VaR P90 de R$ 20,5 milhões" é uma grandeza financeira que o conselho já sabe avaliar e comparar com outras exposições do portfólio.

O que este whitepaper cobre

- Por que indicadores técnicos não sustentam decisões de capital.
- Onde heat maps qualitativos e scores externos de postura param.
- A metodologia FAIR aplicada ao contexto regulatório brasileiro.
- O modelo quantitativo da CSURFACE, com um exemplo integralmente calculado.

O CENÁRIO · PARTE 01

Dois idiomas, uma mesma decisão

Por que a segurança e o conselho não se entendem — e o que essa lacuna custa à organização.

O IDIOMA DA SEGURANÇA

Indicadores técnicos

- CVEs abertas
- CVSS
- MTTR
- Cobertura de scans
- Postura de controles

→

O IDIOMA DO CONSELHO · CRQ TRADUZ

Grandezas financeiras de decisão

- Perda anual esperada (ALE)
- Value at Risk · P90 / P99
- Exposição em reais
- Apetite de risco
- Reserva de capital
- Custo-benefício de remediação

O indicador técnico não chega à mesa de decisão

A equipe de segurança opera com indicadores técnicos — número de CVEs abertas, tempo médio de remediação, número de scans, percentual de cobertura. Eles são essenciais para a gestão do dia a dia. Mas não respondem às perguntas que definem o programa:

- O **comitê de auditoria** precisa avaliar se o programa de segurança é adequado ao risco do negócio.
- O **conselho** precisa aprovar um orçamento de segurança proporcional à exposição real.
- O **CFO** precisa dimensionar reservas de capital para risco cibernético.
- A **corretora de seguro cibernético** precisa quantificar a exposição para precificar a apólice.
- A **auditoria externa** avalia o programa sob frameworks como o COSO ERM.

Nenhuma dessas perguntas se responde com "temos 47 críticas". Todas se respondem com um valor financeiro.

O que a ausência de quantificação produz

1. **Subinvestimento crônico.** O conselho prioriza o que entende. Sem um valor financeiro associado ao risco cibernético, o orçamento de segurança compete em desvantagem com iniciativas que já chegam quantificadas.
2. **Decisões de risco arbitrárias.** Sem quantificação, aceitar ou tratar um risco resulta de julgamento não documentado — sem o trade-off explícito entre o custo da remediação e o custo esperado do incidente.
3. **Seguro cibernético mal precificado.** Sem quantificação própria, a empresa aceita a premissa de pior caso da corretora — e paga prêmio por uma cobertura desalinhada da exposição real.

A lacuna tem custo direto. O custo médio de uma violação de dados no Brasil chegou a **R$ 7,19 milhões** em 2025 (IBM Cost of a Data Breach 2025), e a sanção administrativa da LGPD pode alcançar 2% do faturamento, limitada a R$ 50 milhões por infração. Sem quantificar essa exposição, a organização não dispõe de critério para avaliar se seu nível de investimento em segurança é adequado, insuficiente ou excessivo — e cada um desses desvios tem consequências financeiras distintas e mensuráveis.

Por que isso importa. Risco que não tem preço não entra no processo de decisão de capital. Ele fica fora do orçamento, fora do mapa de riscos corporativos e fora da pauta do conselho — o que significa que a organização não pode gerenciá-lo com a mesma disciplina aplicada aos demais riscos do negócio.

LIMITAÇÕES ATUAIS · PARTE 02

O heat map é opinião colorida, não dado

Por que matrizes qualitativas, scores externos e o CVSS não substituem a quantificação financeira.

Matrizes qualitativas 5×5 não suportam decisão

As matrizes de risco vermelho-amarelo-verde são populares por serem simples. Essa simplicidade, porém, esconde quatro limitações estruturais:

ATENÇÃO **Ambiguidade**
"Probabilidade alta" significa 30% ou 70%? A definição varia entre participantes, e a matriz não dispõe de mecanismo para resolver essa divergência.

ATENÇÃO **Não permitem comparação**
Dois riscos "altos" não são equivalentes — mas a matriz os trata como iguais.

CRÍTICO **Não agregam**
Dois "altos" não somam de forma coerente para "muito alto". Não há aritmética por trás das cores.

CRÍTICO **Não conectam a apetite de risco**
O conselho consegue dizer que não tolera perda de R$ 100 milhões. Não consegue dizer que não tolera "vermelho".

O ponto. Um heat map comunica prioridade relativa entre riscos já conhecidos. Não comunica magnitude, não permite trade-off de capital e não dialoga com o apetite de risco do conselho. Para a mesa de decisão, é um ponto de partida — nunca o destino.

Outros proxies — e onde cada um para

Duas outras abordagens são comuns. Ambas têm valor, e ambas têm um limite claro.

1. **Scores externos de postura.** Notas de 0 a 1000 baseadas em sinais visíveis — certificados, configurações, exposições — são úteis para benchmarking. Mas não traduzem em reais, ignoram a criticidade do ativo e o contexto regulatório, e não respondem "quanto investir?".
2. **O CVSS como medida de risco.** O CVSS quantifica severidade técnica teórica. Uma nota 9.8 em uma máquina de teste sem dados não é o mesmo risco que 9.8 em um servidor de produção com dados de cartão — e o CVSS, sozinho, atribui o mesmo número a ambos.

Nenhum desses instrumentos é dispensável — todos alimentam o modelo de quantificação. O erro é tratar qualquer um deles como a resposta financeira que o conselho espera.

A ABORDAGEM CSURFACE · PARTE 03

FAIR: decompor o risco para poder calculá-lo

O princípio do FAIR e os dados que a plataforma usa para alimentar cada variável do modelo.

A DECOMPOSIÇÃO DO FAIR · DO RISCO OPACO À VARIÁVEL CALCULÁVEL

1 **Risco**
Probabilidade × Magnitude — o todo, decomposto em dois fatores.

→

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

→

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

→

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

O princípio: separar e quantificar

O FAIR — Factor Analysis of Information Risk — é um padrão aberto que decompõe o risco em variáveis observáveis, em vez de tratá-lo como um todo opaco. A estrutura é a do diagrama acima:

Risco = Probabilidade × Magnitude
Probabilidade = Frequência de ameaça × Vulnerabilidade
Magnitude = Perda primária + Perda secundária

Cada variável é estimada como uma **distribuição de probabilidade** — o que reconhece a incerteza inerente e permite a simulação de Monte Carlo. A perda primária é o custo direto do incidente; a secundária inclui multas, perda de clientes e dano de marca.

O FAIR não substitui o julgamento técnico — ele o organiza. Cada estimativa fica explícita, auditável e revisável.

O que alimenta o modelo

O CRQ da CSURFACE não requer que a organização estime parâmetros sem base empírica. O modelo é alimentado pelos dados que a própria plataforma já coleta de forma contínua:

- **Telemetria técnica.** Número de ativos, vulnerabilidades e criticidade — em tempo real, vindos da descoberta contínua da plataforma.
- **Telemetria de ameaça.** O *threat sensor* da CSURFACE vai além dos scores estáticos de CVSS e dos índices de probabilidade de exploração e catálogos de exploração ativa: observa atividade de ameaças, tentativas de exploração, inteligência de exploits e indicadores de campanha — sinais em tempo real que calibram a frequência de eventos no modelo.
- **Contexto de negócio.** Setor, faturamento e número de colaboradores, usados para calibrar probabilidade e magnitude com referências de mercado.
- **Histórico de incidentes.** Eventos da própria organização, quando existem, somados a referências setoriais públicas.
- **Postura de controles.** Cobertura de logs, MFA, ciclo de patches e backups — fatores que modulam a probabilidade.

A precisão do modelo cresce proporcionalmente à abrangência e à atualidade da telemetria coletada. A calibragem é contínua — não um exercício anual de estimativa pontual.

O modelo é alimentado por evidência, não por suposição. Os ativos, as vulnerabilidades e a criticidade que entram no cálculo de risco vêm da descoberta contínua da própria plataforma CSURFACE — a mesma que, em 68 organizações, mapeou **122 mil ativos externos** e, em 16 análises detalhadas, **2.361 vulnerabilidades**. A quantificação é tão sólida quanto o inventário que a sustenta.

A ABORDAGEM CSURFACE · PARTE 03

O modelo, parâmetro por parâmetro

Como probabilidade e magnitude são calculadas, com os multiplicadores calibrados pelo benchmark de 2025.

Probabilidade-base setorial

A chance anual de um incidente material parte de uma referência por setor, ajustada por um multiplicador de maturidade (Básica 1,4× · Intermediária 1,0× · Avançada 0,65×).

SETOR	P(INCIDENTE / ANO)	SETOR	P(INCIDENTE / ANO)
Saúde	**34%**	Telecom	**26%**
Financeiro	**32%**	Educação	**24%**
Governo	**30%**	Indústria	**22%**
Varejo	**28%**	Energia	**20%**

Magnitude — a fórmula do SLE. A perda esperada por evento (Single Loss Expectancy) parte do custo médio nacional e é ajustada por setor, porte e tamanho da superfície:

$$\text{SLE} = \text{R\$ 7,19 mi} \times \text{mult. setorial} \times (\text{faturamento} \div \text{R\$ 200 mi})^{0,35} \times (\text{nº ativos} \div 500)^{0,25}$$

Os expoentes fracionários evitam a linearidade ingênua: dobrar o faturamento não dobra a perda esperada.

Multiplicadores de custo por setor

Derivados da razão entre o custo médio do setor e a média nacional do IBM Cost of a Data Breach 2025.

SETOR	MULT.	SETOR	MULT.
Saúde	**1,59×**	Telecom	**0,92×**
Financeiro	**1,24×**	Educação	**0,78×**
Serviços	**1,18×**	Varejo	**0,72×**
Energia	**1,00×**	Governo	**0,68×**
Indústria	**0,95×**	Outros	**1,00×**

Referências do IBM 2025: Saúde R$ 11,43 mi; Financeiro R$ 8,92 mi; Serviços R$ 8,51 mi; média nacional R$ 7,19 mi.

Da perda por evento ao número do conselho

- **ALE** = probabilidade ajustada × SLE — a perda anual esperada.
- **VaR P90** = 1,85 × ALE — o percentil 90, usado em decisões de capital.
- **VaR P99** = 3,6 × ALE — o pior caso razoável, para reservas e cobertura de seguro.

APLICAÇÃO · PARTE 04

Do inventário técnico ao número em reais

Um cálculo completo, passo a passo: uma varejista de R$ 1,2 bilhão de faturamento.

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

O cenário e o cálculo

Uma varejista omnichannel, faturamento de **R$ 1,2 bilhão**, 4.500 colaboradores, **8.700 ativos** descobertos pela plataforma e maturidade de segurança intermediária. O modelo percorre cada parâmetro:

- **Probabilidade.** Base do varejo (28%), ajustada por maturidade e pelo porte da superfície — probabilidade ajustada de aproximadamente **56%**.
- **SLE.** R$ 7,19 mi × 0,72 (varejo) × $(1.200 \div 200)^{0,35}$ × $(8.700 \div 500)^{0,25}$ ≈ **R$ 19,8 milhões**.
- **ALE.** 56% × R$ 19,8 mi ≈ **R$ 11,1 milhões** ao ano.
- **VaR P90 / P99.** 1,85 × ALE ≈ **R$ 20,5 mi**; 3,6 × ALE ≈ **R$ 39,9 milhões**.
- **Multa LGPD.** mín(R$ 50 mi; faturamento × 2%) × sensibilidade do varejo (1,3) × probabilidade ≈ **R$ 17,5 milhões**.

O resultado, lado a lado

MÉTRICA	VALOR	PARA QUE SERVE
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

Valores calculados com o modelo recalibrado da CSURFACE, base IBM Cost of a Data Breach 2025.

A linguagem do 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. Reduzir o ALE em 20% exige um investimento incremental cuja relação custo-benefício é favorável." Esta é a formulação que permite ao conselho deliberar com o mesmo rigor aplicado a outros riscos do portfólio.

A ABORDAGEM CSURFACE · PARTE 03

A exposição em reais é uma métrica viva

Como o ALE acompanha cada mudança no inventário e na ameaça — e como o CRQ sustenta a documentação regulatória.

AVALIAÇÃO DE RISCO TRADICIONAL

1x

por ano — um retrato estático que envelhece no dia seguinte ao da entrega.

→

CLOSED-LOOP CRQ DA CSURFACE

24/7

o ALE acompanha cada mudança no inventário, na ameaça e na remediação.

O loop fechado em operação

O CRQ da CSURFACE não é uma calculadora que se roda uma vez. Ele está integrado às demais capacidades da plataforma, e a exposição financeira se recalcula sempre que a realidade muda:

1. **Uma vulnerabilidade crítica é remediada.** A probabilidade ajustada cai e o ALE é recalculado automaticamente no mesmo dia.
2. **Um ativo crítico é descoberto.** A descoberta contínua o adiciona ao escopo, o tamanho da superfície sobe e o SLE é reestimado.
3. **O threat sensor detecta exploração ativa de uma CVE do inventário.** A exploração confirmada eleva a probabilidade, e a exposição é reprecificada para cima.
4. **Uma credencial corporativa vaza.** O monitoramento de credenciais incorpora o impacto adicional ao cálculo de magnitude.

Compatibilidade regulatória

A quantificação financeira é exatamente o que reguladores e frameworks de governança esperam. O CRQ apoia diretamente:

- **BACEN.** Gestão integrada de riscos com quantificação financeira da exposição cibernética.
- **CVM.** Deveres fiduciários de administradores na avaliação e divulgação de riscos materiais.
- **LGPD / ANPD.** Relatórios de impacto à proteção de dados (RIPD) sustentados por dados quantitativos.
- **ISO 27005 e COSO ERM.** Frameworks de gestão de risco plenamente compatíveis com a abordagem FAIR.

Da auditoria à decisão. Porque cada estimativa do modelo é explícita e rastreável, o CRQ produz uma trilha auditável: o comitê de auditoria pode verificar a origem de cada parâmetro, e o conselho recebe um digest mensal com a exposição atualizada — em vez de um relatório anual com dados que já não refletem a realidade operacional.

APLICAÇÃO E RESULTADOS · PARTE 04

Da calculadora pública ao módulo integrado

Da estimativa setorial ao relatório defensável: o percurso de implementação e os entregáveis em cada etapa.

TIME-TO-VALUE · DA ESTIMATIVA SETORIAL AO RELATÓRIO DEFENSÁVEL

1. **Dia 1** — Estimativa imediata pela calculadora pública, sem dados internos.
2. **Semana 1** — A descoberta contínua alimenta o modelo com o inventário real de ativos.
3. **Semana 2** — O threat sensor — exploração observada e inteligência de exploits — calibra a probabilidade.
4. **Mês 1** — Primeiro relatório executivo de CRQ, pronto para o comitê de auditoria.
5. **Mês 3+** — Loop fechado em regime: o ALE flutua diariamente e gera digest mensal.

Dois pontos de entrada

O CRQ disponibiliza duas modalidades de uso. A primeira opera exclusivamente com parâmetros setoriais públicos:

- **A calculadora pública de risco.** Disponível em csurface.io, estima ALE e VaR do setor a partir de poucos parâmetros — faturamento, setor, número de colaboradores e ativos. É a porta de entrada: uma primeira leitura de exposição em segundos, sem cadastro.
- **O módulo CRQ integrado.** A versão completa, dentro da plataforma. Substitui as estimativas setoriais pelo inventário real da organização, descoberto e classificado de forma contínua, e mantém o loop fechado de recálculo.

A calculadora dá a ordem de grandeza. O módulo integrado dá o número defensável diante de uma auditoria.

O que cada etapa entrega

Calculadora pública — ordem de grandeza
Uma primeira leitura de exposição em segundos, sem cadastro nem dados internos.

ATENÇÃO **Inventário real — substitui a estimativa**
A descoberta contínua troca referências setoriais pelo inventário descoberto e classificado.

ATENÇÃO **Calibragem por ameaça — probabilidade real**
O threat sensor ajusta a probabilidade pela exploração observada e pela inteligência de exploits, substituindo scores estáticos por evidência operacional.

CRÍTICO **Relatório CRQ — número defensável**
ALE e VaR rastreáveis, prontos para a pauta do comitê e para a auditoria externa.

O que muda na sala do conselho. O risco cibernético deixa de ser um item técnico apresentado uma vez por ano e passa a ser uma linha quantificada do mapa de riscos corporativos — comparável, agregável e diretamente ligada ao apetite de risco aprovado pelo conselho.

PRÓXIMOS PASSOS

A próxima reunião de risco pode começar com um número em reais

O Cyber Risk Quantification é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Em uma plataforma integrada, 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 100% externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM para organizações que necessitam de visibilidade aprofundada dessas camadas.

Use a calculadora de risco

Estime o ALE e o VaR do seu setor em segundos, sem cadastro — a porta de entrada para a quantificação financeira de risco.

Conheça o módulo CRQ

Em uma demonstração, veja a análise FAIR aplicada ao inventário real da organização, com o loop fechado de recálculo contínuo do ALE.

Leia o whitepaper de Threat Intelligence

Priorização dinâmica de vulnerabilidades — um dos insumos críticos para o cálculo de probabilidade do CRQ.

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

Receber análise preliminar gratuita