ÁREA TEMÁTICA: Finanças (ENANGRAD Pleno)

TÍTULO DO TRABALHO: ADAPTAÇÃO DO VALUE-AT-RISK À MENSURAÇÃO DO RISCO CIBERNÉTICO: EVIDÊNCIAS DO VERIS COMMUNITY DATABASE (VCDB)

Resumo

No cenário atual, a quantificação do risco cibernético tornou-se um desafio gerencial em razão da escassez de dados monetários completos, da subnotificação de incidentes e da necessidade de converter eventos técnicos em estimativas financeiras comparáveis. Este trabalho adapta modelos quantitativos de risco financeiro à mensuração exploratória do risco cibernético a partir de registros históricos do VERIS Community Database (VCDB) no período de 2002 a dezembro de 2025. O objetivo é estimar perdas potenciais e métricas de Value-at-Risk (VaR) por categorias de incidente de segurança, como hacking, malware, social, misuse, error e physical, avaliando diferenças de perfil de risco entre elas. O método combina modelagem de frequência com distribuição Binomial Negativa, modelagem de severidade financeira com distribuição Lognormal ajustada ao campo impact.overall_amount, tratamento de outlier extremo, imputação de valores ausentes e simulação de Monte Carlo para gerar distribuições de perda agregada anual e calcular VaR em diferentes níveis de confiança. Os resultados mostram que a imputação Lognormal elevou a perda média anual esperada de aproximadamente US$ 809 milhões para US$ 12,2 bilhões, evidenciando que a ausência de valores monetários subdimensiona o risco; categorias como Hacking e Error concentram maiores perdas de cauda, enquanto Social apresenta impacto relativo menor. As principais contribuições residem em propor uma estrutura quantitativa replicável baseada em dados abertos, demonstrar a viabilidade de comparar perfis de risco financeiro por categoria de incidente e explicitar as limitações informacionais do VCDB para a operacionalização empírica de métricas como Cy-VaR e CVaR, tratadas neste estudo como referências conceituais.

Palavras-chave: risco cibernético; Value-at-Risk; VCDB; simulação de Monte Carlo; modelagem de frequência e severidade.

Abstract

In the current context, cyber risk quantification has become a managerial challenge due to the scarcity of complete monetary data, the underreporting of incidents, and the need to convert technical events into comparable financial estimates. This study adapts quantitative financial risk models to the exploratory measurement of cyber risk, using historical records from the VERIS Community Database (VCDB) covering the period from 2002 to December 2025. The objective is to estimate potential losses and Value-at-Risk (VaR) metrics across different categories of security incidents — hacking, malware, social, misuse, error, and physical — while assessing differences in their respective risk profiles. The method combines frequency modeling with a Negative Binomial distribution, financial severity modeling with a Lognormal distribution fitted to the impact.overall_amount field,

treatment of an extreme outlier, imputation of missing monetary values, and Monte Carlo simulation to generate annual aggregate loss distributions and compute VaR at multiple confidence levels. The results show that Lognormal imputation increased the expected mean annual loss from approximately USD 809 million to USD 12.2 billion, indicating that the absence of monetary values substantially underestimates cyber risk exposure. Categories such as Hacking and Error concentrate higher tail losses, whereas Social presents comparatively lower relative financial impact. The main contributions of this study are the proposal of a replicable quantitative framework grounded in open data, the demonstration that financial risk profiles can be compared across incident categories, and the identification of informational limitations in the VCDB for the empirical operationalization of metrics such as Cy-VaR and CVaR, which are treated in this study as conceptual references.

Keywords: *cyber risk; Value-at-Risk; VCDB; Monte Carlo simulation; frequency-severity modeling*.

1. Introdução

A mensuração do risco em segurança da informação é relevante diante das limitações de abordagens qualitativas e da dificuldade de estimar objetivamente as perdas associadas a incidentes. Nesse contexto, o Value-at-Risk (VaR), amplamente empregado no campo financeiro, surge como alternativa quantitativa para estimar perdas potenciais em determinado horizonte temporal e nível de confiança (Ozcelik & Rees, 2005). Sua aplicação à segurança da informação foi explorada por Orlando (2021), com o Cyber Value-at-Risk (Cy-VaR); por Erola et al. (2022), com um sistema de Cyber-Value-at-Risk (CVaR) baseado em simulações de ativos, ameaças e controles; e por Franco et al. (2024), com o RCVaR, que combina métodos econômicos e dados empíricos de incidentes. Neste artigo, CVaR refere-se ao Cyber-Value-at-Risk, e não ao Conditional Value-at-Risk. Apesar desses avanços, persistem dificuldades para operacionalizar modelos quantitativos em bases abertas, estruturadas e replicáveis.

A quantificação do risco cibernético permanece desafiadora porque os incidentes reportados são heterogêneos, subnotificados e frequentemente incompletos quanto ao impacto financeiro, reforçando a necessidade de métricas replicáveis para apoiar a gestão e a priorização de controles (Bouveret, 2018; Dacorogna & Kratz, 2023; Shevchenko et al., 2022). Bases abertas como o VCDB possibilitam estudos exploratórios por sua taxonomia padronizada de incidentes reais, embora a baixa disponibilidade de valores monetários exija escolhas metodológicas explícitas de frequência, severidade e perda agregada.

Diante dessa lacuna, este estudo investiga como a adaptação da lógica de frequência, severidade e Value-at-Risk (VaR) pode estimar perdas cibernéticas potenciais por categoria de incidente com base em dados históricos do VERIS Community Database (VCDB). Parte-se da premissa de que a combinação entre modelagem de frequência e severidade e simulação de Monte Carlo permite gerar estimativas comparativas de perda agregada e VaR.

Além desta introdução, a Seção 2 apresenta o referencial teórico, a Seção 3 descreve a metodologia, a Seção 4 expõe e discute os resultados e a Seção 5 reúne as conclusões, limitações e possibilidades de pesquisas futuras.

2. Fundamentação Teórica

2.1 Risco financeiro e Value-at-Risk

O risco financeiro é a possibilidade de perdas econômicas associadas à incerteza sobre eventos futuros. Entre as métricas mais difundidas está o Value-at-Risk (VaR), medida probabilística da perda máxima esperada em determinado horizonte temporal e nível de confiança, que traduz incerteza em um valor monetário associado a um quantil da distribuição de perdas (Olson & Wu, 2017; Erola et al., 2022). No domínio cibernético, eventos operacionais geram perdas financeiras por canais como interrupção de serviços, sanções regulatórias e custos reputacionais, o que aproxima a análise de incidentes das métricas financeiras. Assim, o risco cibernético é tratado como risco operacional, com eventos discretos, heterogêneos e potencialmente severos (Biener et al., 2015; Bouveret, 2018; Romanosky, 2016; Shevchenko et al., 2022).

2.2 Modelagem de frequência e severidade

A modelagem de frequência e severidade trata a perda agregada como resultado de dois processos estocásticos distintos: a frequência de ocorrência e a magnitude das consequências (Franco et al., 2024). A frequência costuma ser modelada por distribuições discretas como a Poisson e, em cenários de sobredispersão, pela Binomial Negativa (Bartoszewicz, 2005). Já a severidade, correspondente ao impacto monetário de cada ocorrência, apresenta forte assimetria à direita e cauda pesada, justificando distribuições como Lognormal, Weibull e Pareto generalizada (Pak, 2014). Como a perda média pouco representa eventos raros e severos, medidas baseadas em quantis, como VaR a 95% ou 99%, estimam limiares de perda em regiões extremas (Biener et al., 2015; Bouveret, 2018; Kamdem & Kapsa, 2025; Shevchenko et al., 2022).

A frequência determina quantos incidentes ocorrem e a severidade determina o impacto de cada um, permitindo extrair média, dispersão e quantis de cauda da distribuição agregada. A simulação de Monte Carlo integra-se a essa estrutura ao combinar, em iterações sucessivas, incidentes simulados com perdas extraídas da distribuição de severidade, produzindo uma distribuição empírica de perdas agregadas (Erola et al., 2022). Essa decomposição identifica se o risco decorre da recorrência dos eventos, da magnitude das perdas ou da interação entre esses fatores (Adekoya et al., 2025; Franco et al., 2024).

2.3 VCDB

O VERIS Community Database (VCDB) é uma iniciativa aberta e colaborativa de coleta e catalogação de incidentes de segurança publicamente divulgados, estruturada segundo a taxonomia VERIS (VCDB, 2024). Seus registros são organizados em blocos como action, actor, asset, attribute, victim, timeline e impact (VERIS, 2023). Por ser um repositório público, o VCDB está sujeito a subnotificação, heterogeneidade na qualidade dos registros e cobertura desigual entre setores e regiões (VCDB, 2024; VERIS, 2023), além da escassez de informações financeiras estruturadas.

2.4 Trabalhos relacionados

A literatura inclui estudos empíricos, atuariais e econômicos que modelam perdas por frequência, severidade, custos e impacto de mercado. Bouveret (2018) propõe estrutura próxima à Loss Distribution Approach, combinando frequência, severidade, Monte Carlo, VaR e Expected Shortfall. Biener, Eling e Wirfs (2015) evidenciam falta de dados e perdas extremas, enquanto Shevchenko et al. (2022) mostram, com a base Advisen, que frequência e severidade variam por tipo de ameaça, reforçando a necessidade de segmentação por categoria. Outros trabalhos decompõem perdas de vazamentos (Theriot & Gowan, 2023), aplicam estudo de caso bancário (Pollmeier, Bongiovanni & Slapničar, 2023), estimam VaR dinâmico (Dzhamtyrova & Maple, 2021), medem impacto sobre mercados (Celeny et al., 2024), combinam aprendizado de máquina e teoria de valores extremos (Kamdem & Kapsa, 2025) ou tratam de transferência de risco por seguros (Woods & Wolff, 2025).

Entre os modelos de valor em risco, Orlando (2021) propõe o Cy-VaR, dependente de dados sobre ativos, vulnerabilidades e atacantes; Erola et al. (2022) operacionalizam o CVaR por simulação sobre ativos, ameaças, controles e danos; e Franco et al. (2024) introduzem o RCVaR, baseado em dados empíricos setoriais. Este trabalho se aproxima desses estudos, mas se distingue ao usar o VCDB como base aberta, adotando categorias de incidente

como unidade de análise e combinando frequência, imputação Lognormal, Monte Carlo e VaR para comparar perfis de risco.

3. Metodologia

Trata-se de estudo quantitativo, aplicado e exploratório-descritivo. A natureza quantitativa decorre de procedimentos estatísticos e simulação, e o caráter aplicado reside na adaptação de instrumental das finanças à análise do risco cibernético. A dimensão exploratória examina a viabilidade de transpor métodos quantitativos a uma base histórica de incidentes (Gil, 2009), enquanto o caráter descritivo se manifesta na organização e comparação de categorias com base em padrões observados (Lakatos & Marconi, 2003).

As etapas da metodologia estão sintetizadas na Figura 1, em quatro momentos: seleção da base de dados, preparação e modelagem, análise estatística e simulação, e cálculo das métricas de risco.

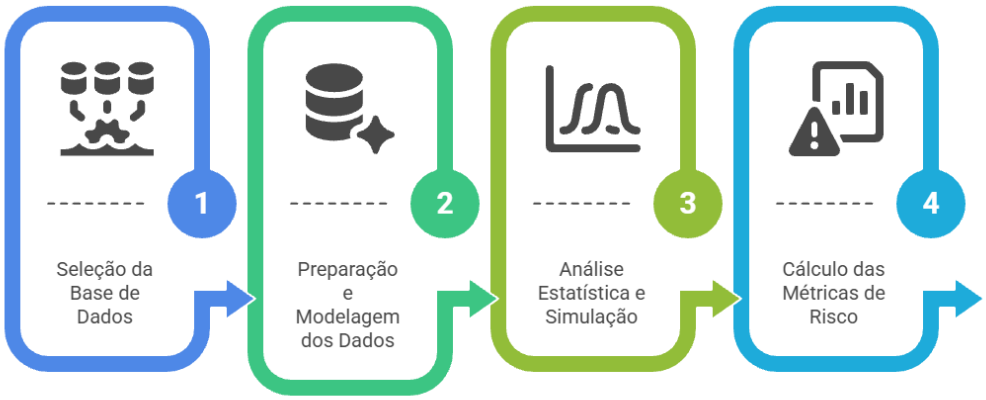

Figura 1 – Etapas da Metodologia
Fonte: Elaborado pelos Autores

3.1 Seleção da base de dados

A base empírica foi o VERIS Community Database (VCDB), em formato JSON, com registros históricos de incidentes divulgados publicamente entre 2002 e dezembro de 2025. A escolha justifica-se pela estrutura padronizada segundo a taxonomia VERIS, que organiza os incidentes em dimensões comparáveis como ação, ator, ativo, vítima, linha do tempo e impacto.

Embora a base bruta contenha registros desde 1971, o recorte de 2002 a 2025 concentrou a análise no intervalo de maior densidade informacional. Foram considerados apenas registros com informação válida sobre categoria e ano de ocorrência, garantindo consistência mínima para a comparação entre categorias.

3.2 Preparação e modelagem dos dados

Essa etapa compreendeu a leitura do dataset JSON, identificação das categorias, extração dos campos relevantes e conversão em variáveis analíticas: o que ocorreu (action.<categoria>.variety), quanto foi perdido (impact.overall_amount), quando ocorreu (timeline.incident.year) e como ocorreu (summary), além de campos contextuais actor., victim. e asset.*.

A modelagem concentrou-se nas categorias hacking, malware, social, misuse, error e physical. O campo impact.overall_rating foi descartado por insuficiência de dados válidos, e incidentes em múltiplas categorias foram contabilizados em todas elas, o que pode ampliar artificialmente a frequência e deve ser considerado na interpretação dos resultados.

3.3 Análise estatística e simulação

Essa etapa modelou separadamente a frequência de incidentes e a severidade financeira das perdas, com análise exploratória prévia da distribuição dos incidentes, disponibilidade de valores monetários e comportamento das variáveis de impacto, em dólares e escala logarítmica, segmentada por categoria.

A implementação foi feita em Jupyter no Google Colab, em Python, com pandas, numpy, random, scipy.stats, matplotlib e seaborn, e semente aleatória fixa igual a 42 para reprodutibilidade. A frequência anual foi modelada por categoria, calculando-se média e variância de cada série histórica. Devido à sobredispersão observada, adotou-se a distribuição Binomial Negativa, com parâmetros estimados pelas relações p = média/variância e r = média²/(variância − média). As contagens anuais do VCDB refletem o processo de divulgação e curadoria da base, não a taxa real de ocorrência.

A severidade financeira foi modelada a partir dos registros com valores válidos em impact.overall_amount. Um valor extremo de US$ 1 trilhão foi identificado e mantido na caracterização descritiva, mas excluído do ajuste da distribuição e da simulação para reduzir sua influência desproporcional. Adotou-se a distribuição Lognormal para o impacto financeiro individual, ajustada globalmente sem segmentação por categoria, sob a hipótese de que ela poderia aproximar a severidade dos casos sem valor reportado. Assim, as diferenças entre categorias nas métricas simuladas decorrem predominantemente das distribuições de frequência.

Na simulação de Monte Carlo, em cada uma das 10.000 iterações sorteou-se a quantidade anual de incidentes por categoria (Binomial Negativa) e, para cada incidente, uma perda individual (Lognormal), somando-se as perdas para gerar a perda agregada anual. Calcularam-se perda média esperada, desvio-

padrão e quantis de cauda para estimar o VaR a 95% e 99%, comparando-se cenários apenas com registros monetizados e com imputação Lognormal.

Como incidentes podem pertencer a mais de uma categoria, a perda total agregada soma contribuições múltiplas vezes, devendo ser interpretada como índice comparativo entre cenários, não como estimativa da perda anual da base.

3.4 Cálculo das métricas de risco e comparação

As distribuições simuladas foram usadas para calcular perda média esperada, desvio-padrão e VaR a 95% e 99%, por categoria e para o conjunto agregado.

O VaR foi operacionalizado como o quantil da distribuição simulada correspondente ao nível de confiança: o VaR 95% representa o limiar abaixo do qual se situam 95% das perdas simuladas, e o VaR 99%, o limiar de 99%, permitindo comparar o risco de cauda entre categorias.

As métricas Cy-VaR e CVaR foram mantidas como referências conceituais, mas não operacionalizadas empiricamente, pois o VCDB não dispõe, de forma integrada, dos dados requeridos por esses modelos, como vulnerabilidades, ativos, atacantes, controles e propagação de impactos.

4. Análise e Discussão dos Resultados

Os resultados são apresentados em correspondência com as etapas metodológicas descritas na Seção 3: caracterização da base, preparação das variáveis, modelagem da severidade financeira, modelagem da frequência anual, simulação de perdas agregadas e cálculo das métricas de risco.

4.1 Caracterização da base e categorias de incidente

A base de dados VCDB, em formato JSON, reúne 10.037 registros de incidentes de segurança, distribuídos principalmente entre as categorias hacking (33,48%) e error (26,71%), seguidas por misuse (17,82%), malware (16,38%), physical (16,20%) e social (6,40%). Conforme demonstrado na Figura 2, essa distribuição evidencia a predominância de algumas categorias e sugere perfis distintos de ocorrência entre os tipos de incidente.

4.2 Disponibilidade dos dados financeiros e preparação das variáveis

No que se refere à disponibilidade de dados financeiros, a análise exploratória revelou que apenas 3,23% dos registros, correspondentes a 324 de 10.037 incidentes, continham valores financeiros informados no campo impact.overall_amount.

Ainda conforme apresentado na Figura 2, a estatística descritiva desses valores indicou uma distribuição de perdas assimétrica e de cauda pesada,

característica comum em riscos operacionais e cibernéticos, com mediana de US$ 250.000 e média de US$ 3,1 bilhões, fortemente influenciada por eventos extremos, entre os quais se destaca um valor máximo reportado de US$ 1 trilhão. Esse valor foi considerado na caracterização exploratória da base, mas tratado como outlier extremo nas etapas de ajuste da severidade e simulação, conforme descrito na metodologia. Por sua vez, a variável impact.overall_rating foi desconsiderada nas etapas subsequentes, uma vez que apresentou baixa disponibilidade informacional, com apenas 237 registros não nulos ou diferentes de unknown, o que comprometeria sua utilização analítica.

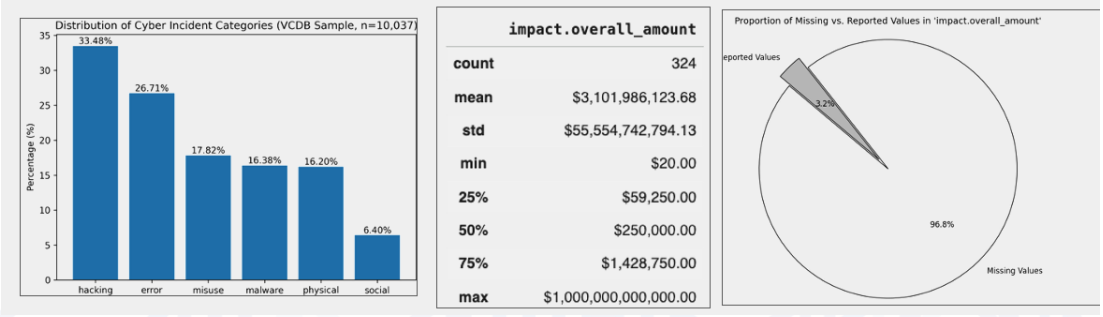

Figura 2 – A: Distribuição das categorias de incidentes cibernéticos no VCDB; B: Estatísticas descritivas; C: Proporção de valores ausentes e reportados no atributo "impact.overall_amount".

Fonte: Elaborado pelos Autores

4.3 Modelagem da severidade financeira

Após a aplicação da transformação logarítmica de base 10 aos valores não nulos, observou-se redução da assimetria da distribuição e maior aproximação a um comportamento compatível com a normalidade. Com base nessa inspeção exploratória dos dados transformados, adotou-se a distribuição Lognormal como aproximação para a modelagem da severidade do impacto, conforme ilustrado na Figura 3.

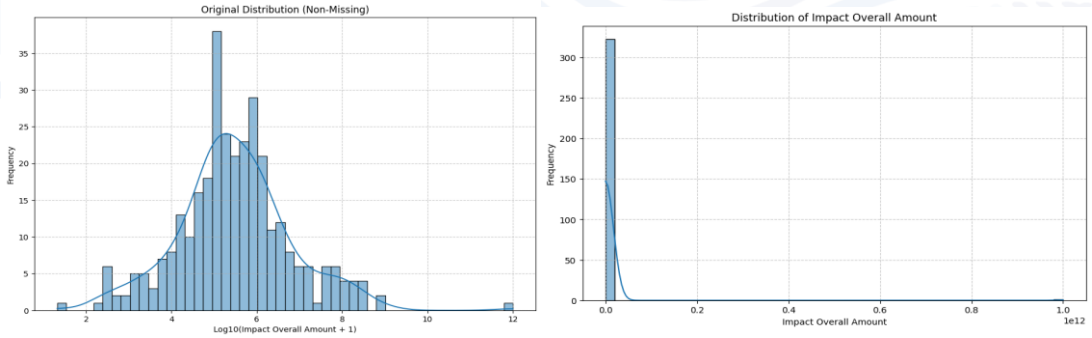

Figura 3 – A: Distribuição dos valores registrados no atributo impact.overall_amount; B: Distribuição dos valores não ausentes do atributo.

Fonte: Elaborado pelos Autores

A Figura 4 apresenta a distribuição do impacto financeiro, em dólares norte-americanos e em escala logarítmica, segmentada pelas categorias de

incidentes do framework VERIS. A análise dos boxplots revela acentuada heterogeneidade na magnitude dos impactos, com caudas longas e outliers extremos em todas as classes; embora as medianas apresentem relativa convergência, as categorias Hacking e Social destacam-se pela maior dispersão interquartílica e frequência de eventos de alta severidade, enquanto Error e Physical concentram incidentes em patamares financeiros inferiores.

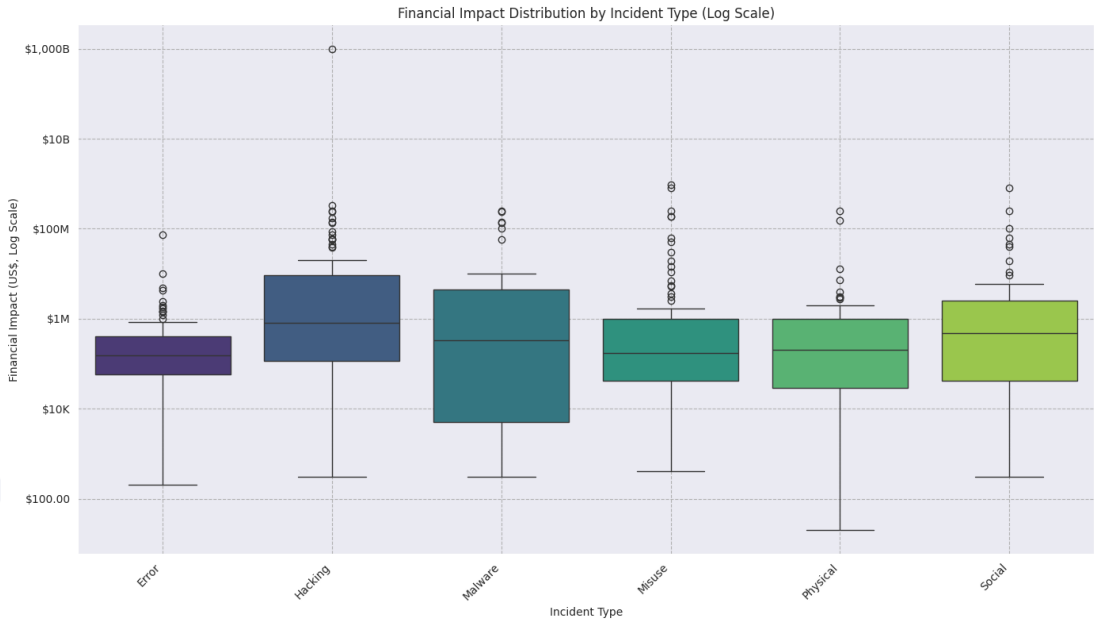

Figura 4 – Distribuição do impacto financeiro por tipo de incidente.

Fonte: Elaborado pelos Autores

Os parâmetros da distribuição Lognormal foram ajustados a partir dos registros contendo impacto financeiro válido no campo impact.overall_amount, após a exclusão do valor extremo de US$ 1 trilhão identificado na análise exploratória. Assumiu-se, como hipótese de trabalho, que a distribuição dos valores monetários observados poderia servir como aproximação da severidade dos casos sem valor reportado. Essa premissa é restritiva e constitui limitação central do estudo, especialmente porque a heterogeneidade de severidade entre categorias, visível na Figura 4, não foi incorporada à simulação, que empregou uma única distribuição de severidade. A segmentação da Lognormal por categoria constitui refinamento natural para trabalhos futuros.

4.4 Modelagem de frequência anual

Para cada categoria de incidente, construiu-se uma série de contagem anual com base no ano de ocorrência registrado no VCDB. A análise dessas séries indicou sobredispersão significativa, com variância superior à média em todas as categorias analisadas. Por essa razão, a distribuição Binomial Negativa foi adotada em detrimento da distribuição de Poisson para representar a frequência anual de incidentes, conforme ilustrado na Figura 5.

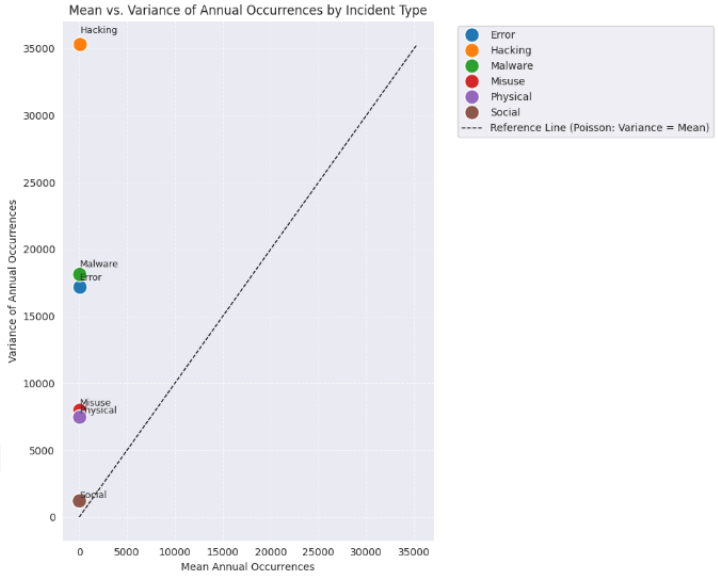

Figura 5 – Média versus variância segundo os tipos de incidente.

Fonte: Elaborado pelos Autores

4.5 Simulação de perdas agregadas anuais

A distribuição original dos dados reais evidenciou assimetria e cauda pesada, características de perdas financeiras extremas. A distribuição simulada, gerada pela imputação Lognormal, replicou o comportamento geral da distribuição original, preservando a extensão da cauda pesada, conforme ilustrado na Figura 6.

A Figura 7 compara a distribuição do impacto financeiro considerando os dados combinados, após imputação, e os dados originais registrados no campo impact.overall_amount.

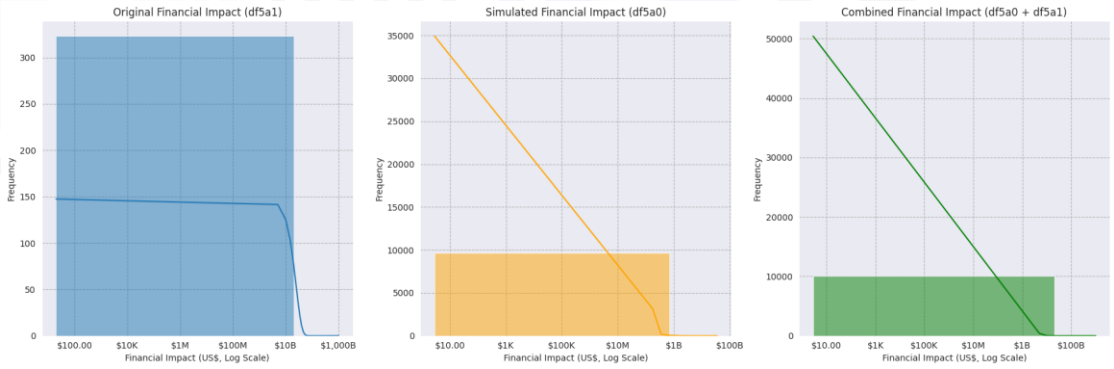

Figura 6 – A: Impacto financeiro dos dados originais; B: Impacto financeiro simulado; C: Impacto financeiro combinado.

Fonte: Elaborado pelos Autores

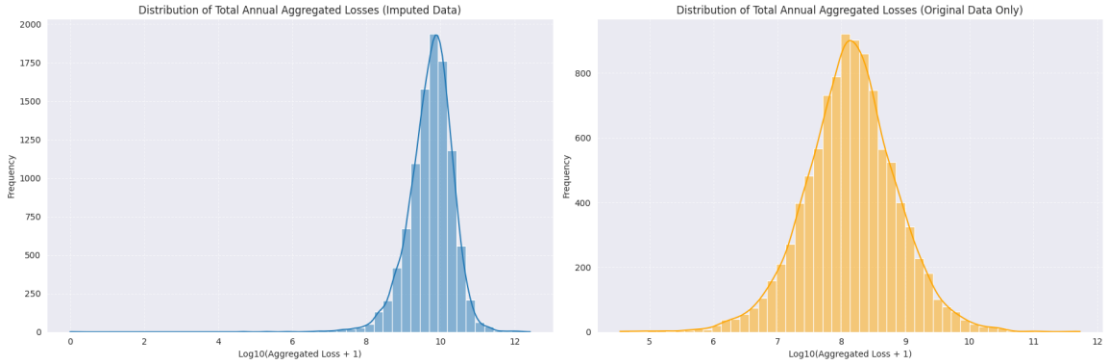

Figura 7 – A: Distribuição do impacto de perdas com dados combinados; B: Distribuição do impacto financeiro com dados originais registrados no campo impact.overall_amount.

Fonte: Elaborado pelos Autores

Considerando apenas os ~3% de registros com impacto observado, a perda média anual esperada foi de US$ 809 milhões; com imputação Lognormal, subiu para US$ 12,2 bilhões. Essa discrepância é cenário de sensibilidade: o aumento decorre da atribuição de perdas aos ~97% de registros sem valor monetário, sob hipótese de mesma distribuição — como a ausência raramente é aleatória, US$ 12,2 bilhões deve ser lido como estimativa exploratória superior. Ainda assim, desconsiderar registros sem valor pode subdimensionar significativamente o risco cibernético.

4.6 Métricas de risco e comparação por categoria

O Value-at-Risk (VaR) foi calculado nos níveis de 95% e 99% para as perdas totais associadas ao atributo impact.overall_amount, evidenciando diferenças entre os cenários com e sem imputação de dados, conforme ilustrado na Tabela 1. No cenário ampliado, o VaR atingiu US$ 38,2 bilhões no nível de 95% e US$ 87,2 bilhões no nível de 99%.

Na decomposição por tipo de incidente, essa assimetria torna-se ainda mais evidente, uma vez que as categorias Hacking e Error concentram os maiores valores de cauda, com VaR a 99% de US$ 40,8 bilhões e US$ 31,0 bilhões, respectivamente. A categoria Malware também apresenta risco de cauda relevante, com VaR a 99% de US$ 27,1 bilhões e o maior desvio-padrão entre as categorias analisadas, indicando elevada volatilidade das perdas simuladas. Em contraste, incidentes da categoria Social apresentam impacto relativo inferior.

Tabela 1 - Medidas de risco por tipo de incidente

Tipo de incidente	Média esperada	VaR 95%	VaR 99%	Desvio-padrão
Hacking	US$ 3,3 bilhões	US$ 14,6 bilhões	US$ 40,8 bilhões	US$ 13,3 bilhões

Tipo de incidente	Média esperada	VaR 95%	VaR 99%	Desvio-padrão
Error	US$ 2,9 bilhões	US$ 11,1 bilhões	US$ 31,0 bilhões	US$ 18,5 bilhões
Malware	US$ 1,8 bilhão	US$ 8,1 bilhões	US$ 27,1 bilhões	US$ 24,3 bilhões
Physical	US$ 1,8 bilhão	US$ 7,1 bilhões	US$ 24,1 bilhões	US$ 13,0 bilhões
Misuse	US$ 1,8 bilhão	US$ 7,6 bilhões	US$ 21,8 bilhões	US$ 9,7 bilhões
Social	US$ 586,5 milhões	US$ 2,4 bilhões	US$ 8,2 bilhões	US$ 3,1 bilhões

Fonte: Elaborado pelos Autores

O Cy-VaR (Orlando, 2021) depende de vulnerabilidades, ativos e atacantes potenciais, e o CVaR (Erola et al., 2022) requer dados integrados de ativos, ameaças, controles e danos. O VCDB não fornece esses arranjos, inviabilizando a operacionalização empírica. A análise concentrou-se, portanto, no VaR simulado, mantendo Cy-VaR e CVaR como referências conceituais para explicitar as limitações informacionais da base.

5. Conclusão e Contribuições

O objetivo deste trabalho foi adaptar a lógica de frequência, severidade e Value-at-Risk à mensuração exploratória do risco cibernético a partir do VCDB. Conclui-se que essa adaptação é viável, condicionada às informações disponíveis na base: a combinação de modelagem de frequência, impacto (impact.overall_amount) e simulação de Monte Carlo permitiu obter distribuições de perdas e métricas de VaR úteis à comparação entre categorias.

A principal contribuição é a proposição de uma estrutura quantitativa replicável, baseada em dados abertos, aproximando finanças quantitativas e segurança da informação. Hacking e Error concentraram os maiores valores de cauda (VaR a 95% e 99%), enquanto Social apresentou menor impacto relativo, confirmando que a abordagem discrimina diferenças relevantes de exposição a perdas extremas.

As principais limitações decorrem da base empírica: a maioria dos registros do VCDB não contém valores monetários, exigindo imputação sob hipótese de ausência aleatória provavelmente violada, e a heterogeneidade de setores restringe inferências específicas. Não foi possível operacionalizar Cy-VaR e CVaR, o uso de impact.overall_rating foi inviável e a exclusão do outlier de US$ 1 trilhão não teve análise de sensibilidade formal.

Como agenda futura, recomenda-se ampliar a investigação com bases complementares, testar modelos alternativos como o RCVaR e avaliar a robustez das estimativas em contextos setoriais ou nacionais.

Referências

ADEKOYA, Olumayowa Adefowope; ATLAM, Hany F.; LALLIE, Harjinder Singh. Quantifying the multidimensional impact of cyber-attacks in digital financial services: a systematic literature review. **Sensors**, v. 25, n. 14, p. 4345, 2025.

BARTOSZEWICZ, B. Modelling the claim count with Poisson regression and negative binomial regression. p. 103–110, 2005. Disponível em: https://doi.org/10.1007/3-540-26981-9_13.

BIENER, C.; ELING, M.; WIRFS, J. H. Insurability of cyber risk: an empirical analysis. **Geneva Papers on Risk and Insurance-Issues and Practice**, v. 40, n. 1, p. 131–158, 2015. Disponível em: https://doi.org/10.1057/GPP.2014.19.

BOUVERET, Antoine. Cyber risk for the financial sector: a framework for quantitative assessment. IMF Working Paper, WP/18/143. Washington, DC: International Monetary Fund, 2018.

CELENY, Daniel; MARÉCHAL, Loïc; ROUSSELOT, Evgueni; MERMOUD, Alain; HUMBERT, Mathias. Prioritizing investments in cybersecurity: empirical evidence from an event study on the determinants of cyberattack costs, 2024.

DACOROGNA, Michel; KRATZ, Marie. Managing cyber risk, a science in the making, 2023.

DZHAMTYROVA, Raisa; MAPLE, Carsten. Dynamic cyber risk estimation with competitive quantile autoregression, 2021.

EROLA, Arnau; AGRAFIOTIS, Ioannis; NURSE, Jason R. C.; AXON, Louise et al. A system to calculate cyber value-at-risk. **Computers & Security**, v. 113, p. 102545, 2022.

FRANCO, Muriel Figueredo; KÜNZLER, Fabian; VON DER ASSEN, Jan; FENG, Chao et al. RCVaR: an economic approach to estimate cyberattacks costs using data from industry reports. **Computers & Security**, 2024.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.

KAMDEM, Jules Sadefo; KAPSA, Danielle Selambi. CyberRisk prediction using machine learning and extreme value theory. Preprint/manuscript, 2025.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

OLSON, David L.; WU, Desheng Dash. **Enterprise risk management models**. Springer, 2017.

ORLANDO, Albina. Cyber risk quantification: investigating the role of cyber value at risk. **Risks**, v. 9, n. 10, p. 184, 2021.

OZCELIK, Y.; REES, J. A new approach for information security risk assessment: value at risk. **Social Science Research Network**, 2005. Disponível em: https://doi.org/10.2139/SSRN.1104264.

PAK, R. J. Estimating loss severity distribution: convolution approach. **Journal of Mathematics and Statistics**, v. 10, n. 2, p. 247–254, 2014. Disponível em: https://doi.org/10.3844/JMSSP.2014.247.254.

POLLMEIER, Santiago; BONGIOVANNI, Ivano; SLAPNIČAR, Sergeja. Designing a financial quantification model for cyber risk: a case study in a bank. Safety Science, v. 159, p. 106022, 2023. Disponível em: https://doi.org/10.1016/j.ssci.2022.106022.

ROMANOSKY, Sasha. Examining the costs and causes of cyber incidents. **Journal of Cybersecurity**, v. 2, n. 2, p. 121–135, 2016.

SHEVCHENKO, Pavel V.; JANG, Jiwook; MALAVASI, Matteo; PETERS, Gareth W.; SOFRONOV, Georgy; TRÜCK, Stefan. The nature of losses from cyber-related events: risk categories and business sectors. arXiv preprint arXiv:2202.10189, 2022.

THERIOT, Justin; GOWAN, Benjamin. Does decomposing losses improve our understanding of the financial impact of data breaches? Manuscript, 2023.

VCDB. **VERIS Community Database (VCDB)**. 2024. Disponível em: https://verisframework.org/vcdb.html.

VERIS. **The Vocabulary for Event Recording and Incident Sharing (VERIS) - dataset**. 2023. Disponível em: https://github.com/vz-risk/VCDB/blob/master/data/csv/vcdb.csv.zip.

WOODS, Daniel W.; WOLFF, Josephine. A history of cyber risk transfer. Journal of Cybersecurity, v. 11, n. 1, 2025. Disponível em: https://doi.org/10.1093/cybsec/tyae028.