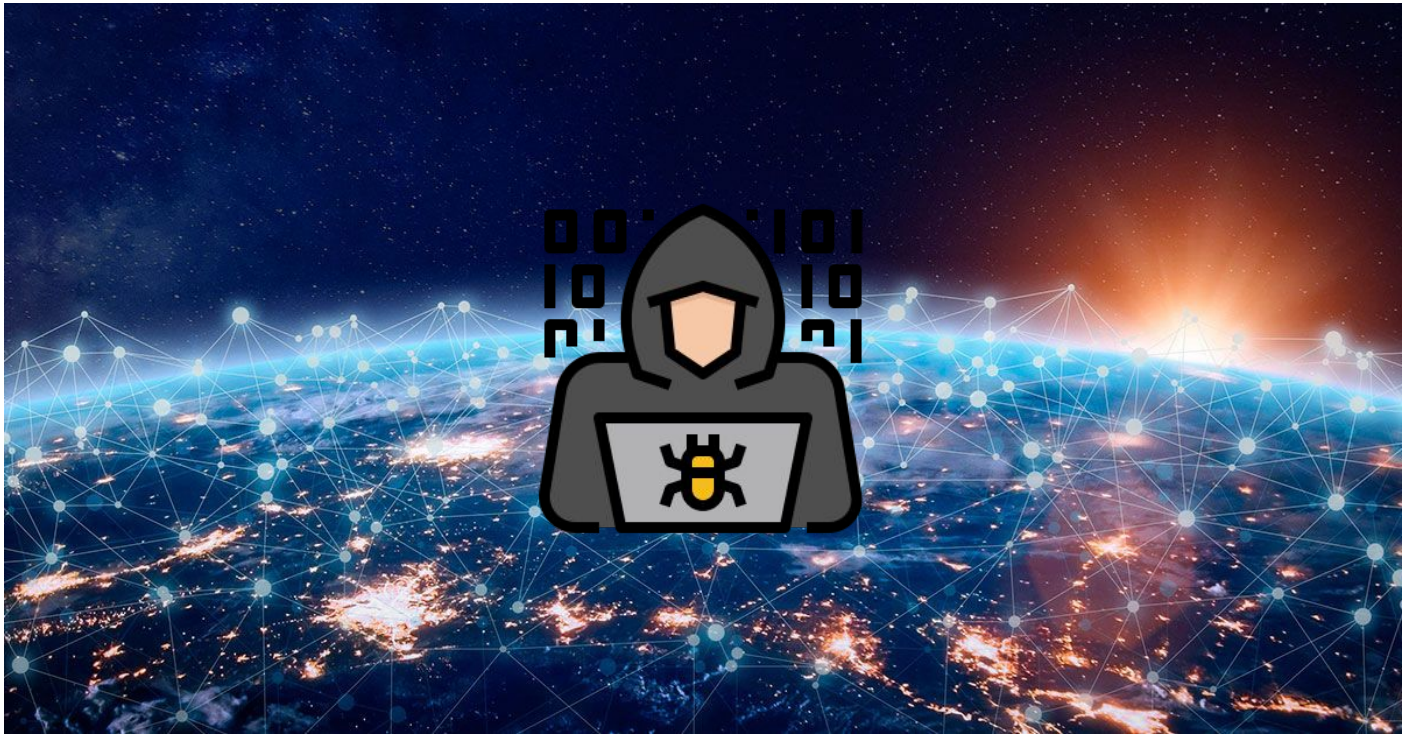
SIM-Ciber: Uma Solução Baseada em Simulações Probabilísticas para Quantificação de Riscos e Impactos de Ciberataques Utilizando Relatórios Estatísticos

João Nunes, Muriel Franco, Eder Scheid, Geancarlo Kozenieski, Henrique Lindemann, Laura Soares, Jéferson Nobre, Lisandro Granville

Universidade Federal do Rio Grande do Sul (UFRGS)

Introdução (1)

Introdução (1)



Introdução (2)

Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano

Fonte: Jornal da USP (2023)

Introdução (2)

Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano

Fonte: Jornal da USP (2023)

Microsoft barra ataque DDoS com tráfego recorde de 3,47 Tb/s contra o alvo

Ataque DDoS com pico de 3,47 Tb/s é o maior já mitigado pela Microsoft; ação ocorreu contra cliente da plataforma Azure

Fonte: Tecnoblog (2022)

Introdução (2)

Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano

Fonte: Jornal da USP (2023)

JBS pagou US$ 11 milhões em resgate a autores de ataque ransomware

Fonte: Exame (2021)

Fonte: Tecnoblog (2022)

Introdução (2)

Brasil sofreu mais de 100 bilhões de tentativas de ataques

Fonte: IBM (2023)

JBS pagou US$ 11 milhões em autores de ataque ransomware

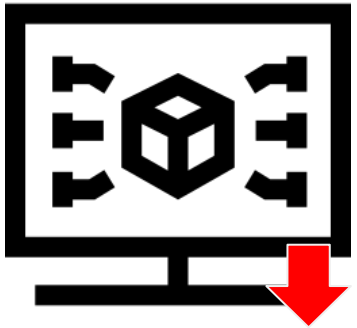
Fonte: Exame (2021)

Fonte: [illegible]og (2022)

Motivação

Aumento no número de ciberataques

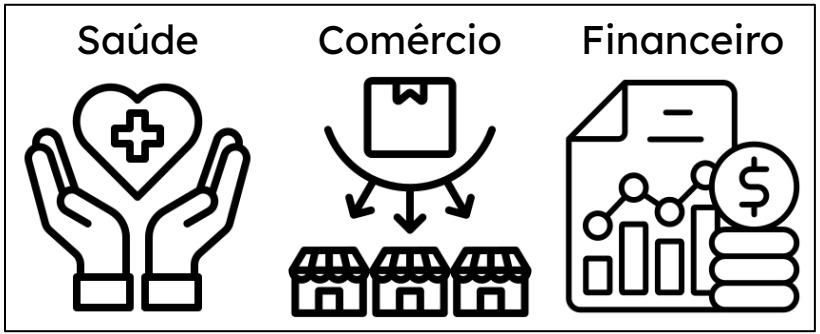
Alto custo decorrente dos ciberataques



Falta de simulações e análise dos riscos e potenciais impactos dos ciberataques utilizando dados reais

Referencial Teórico

SETORES



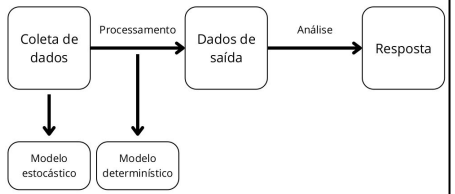
CIBERATAQUES

MÉTODOS PROBABILÍSTICOS

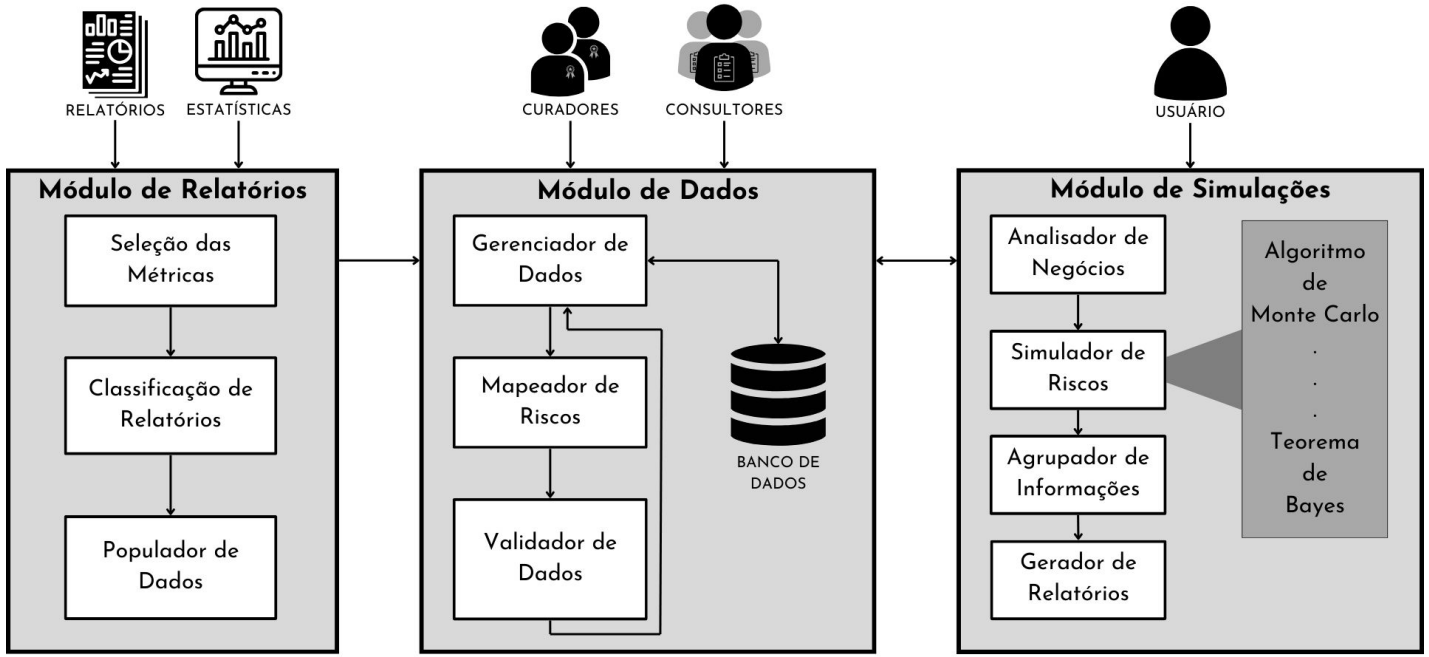
Teorema de Bayes

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

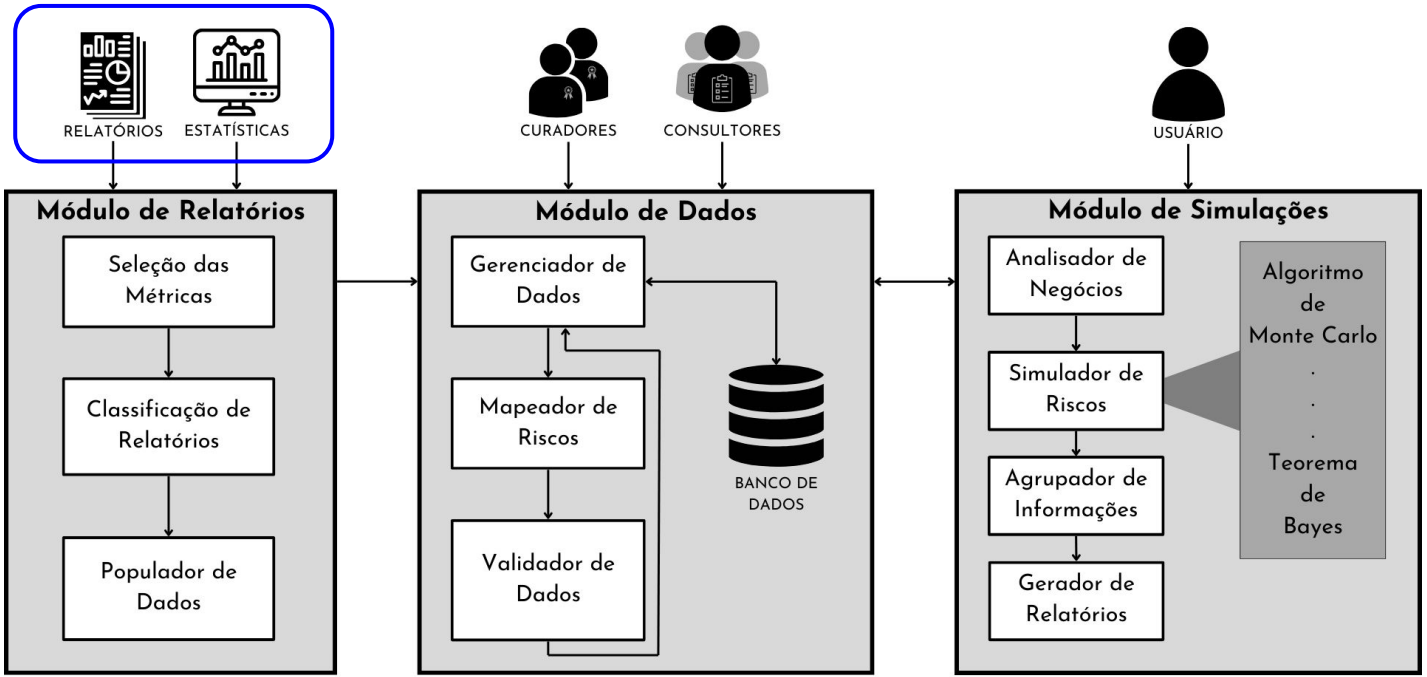
Método de Monte Carlo



SIM-Ciber


RELATÓRIOS
ESTATÍSTICAS
CURADORES
CONSULTORES
USUÁRIO
Módulo de Relatórios
Seleção das Métricas
Classificação de Relatórios
Populador de Dados
Módulo de Dados
Gerenciador de Dados
Mapeador de Riscos
Validador de Dados
BANCO DE DADOS
Módulo de Simulações
Analisador de Negócios
Simulador de Riscos
Agrupador de Informações
Gerador de Relatórios
Algoritmo de Monte Carlo
Teorema de Bayes

Tipos de Dados (1)



Tipos de Dados (2)

Tipos de Dados (3)

- 536 dados tangíveis e não tangíveis

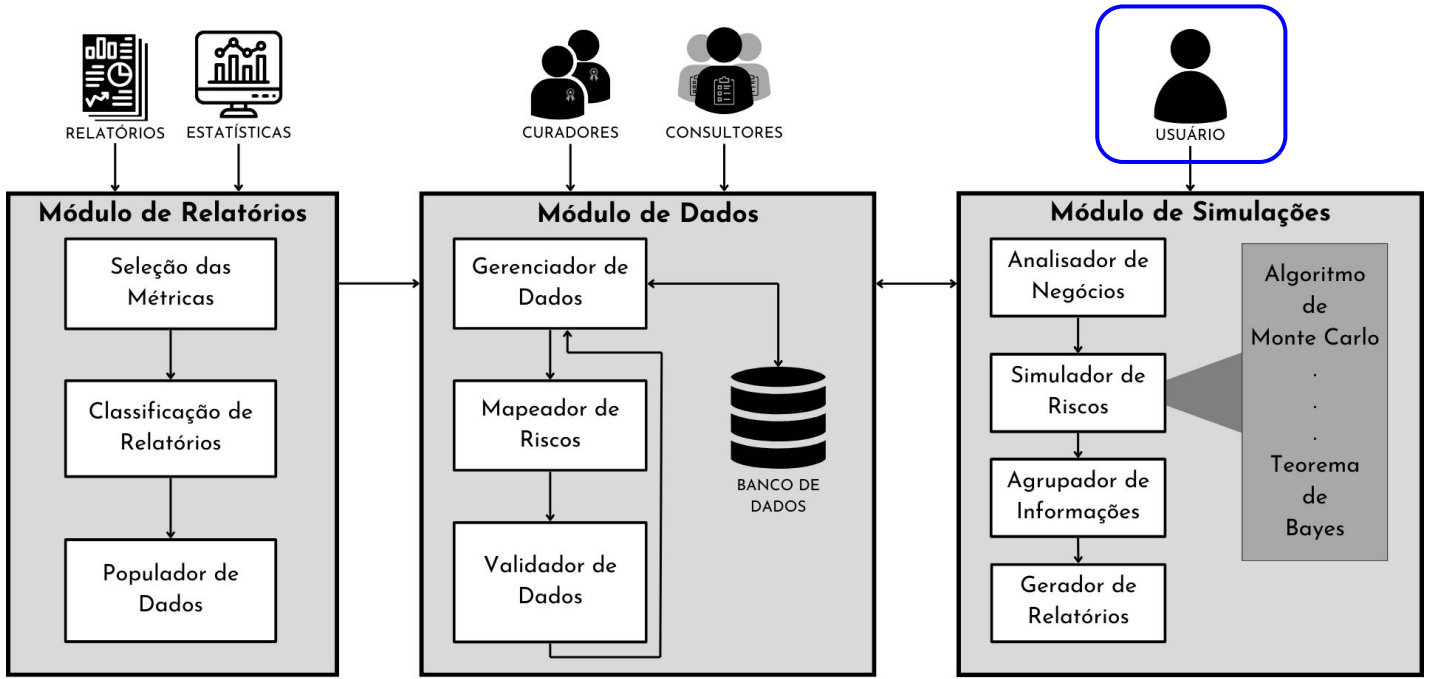
Dados Não Tangíveis

Condição A	Condição B	Probabilidade	Fonte
Malware	Setor de Comércio	21.74%	(FORTINET, 2021)
Ransomware	Setor Financeiro	64%	(SOPHOS, 2023)
Ciberataque	Pequenas e Médias Empresas	43%	(VERIZON, 2023)
DDoS	Brasil	1.75%	(MICROSOFT, 2022)

Dados Tangíveis

Condição A	Condição B	Valor	Métrica	Fonte
Custo	Ransomware	$ 170,404	Valor por Ataque	(SOPHOS, 2021)
Custo | Brecha	Brasil	$ 1.22 M	Valor por Ataque	(IBM, 2023)
Ransomware	-	693.3 M	Ataques por Ano	(SONICWALL, 2023)

Requisições

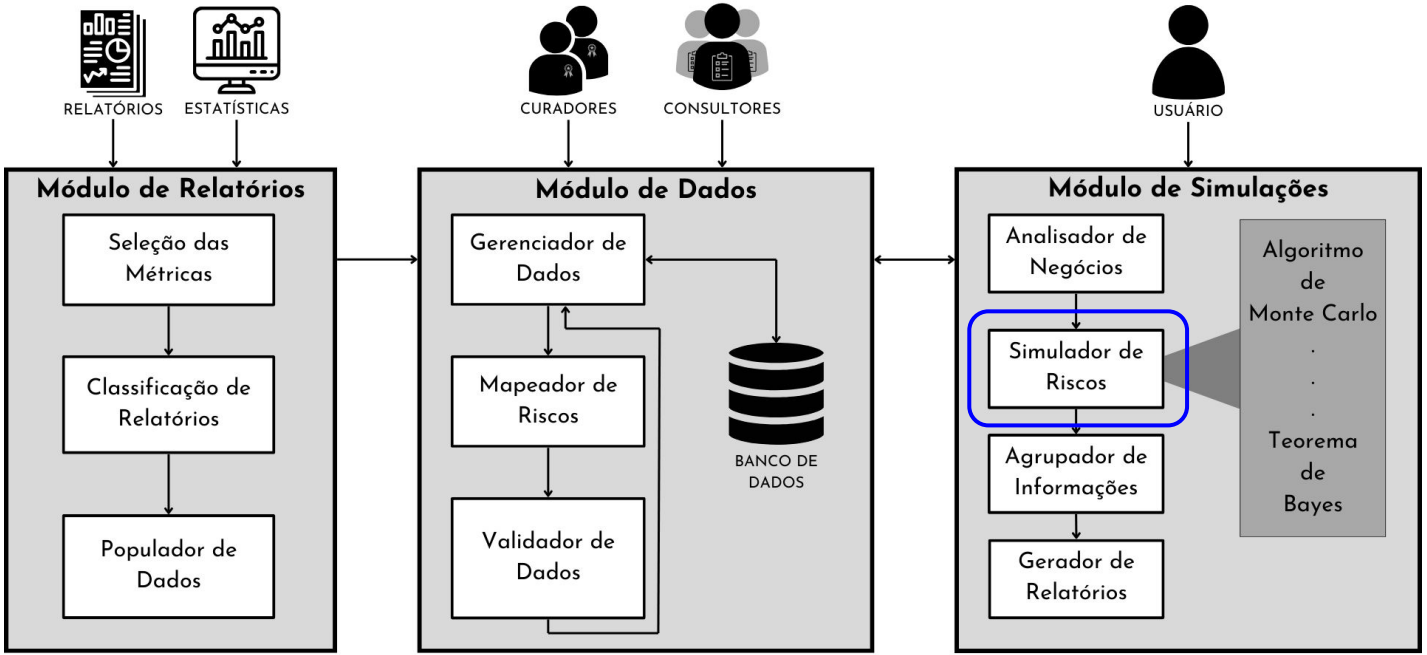


Exemplo de Requisição

Informações na Requisição	Significado
001	Setor da Empresa: Setor de Saúde
110	Tipo de Ataque: Malware e Phishing
0100	Localização Geográfica: LATAM
100	Relevância dos Dados: Todos
Brasil	Informações Extras: Brasil

- Contando com esse exemplo, ao todo são 315 requisições possíveis
    - A partir da variação das flags

Simulações (1)

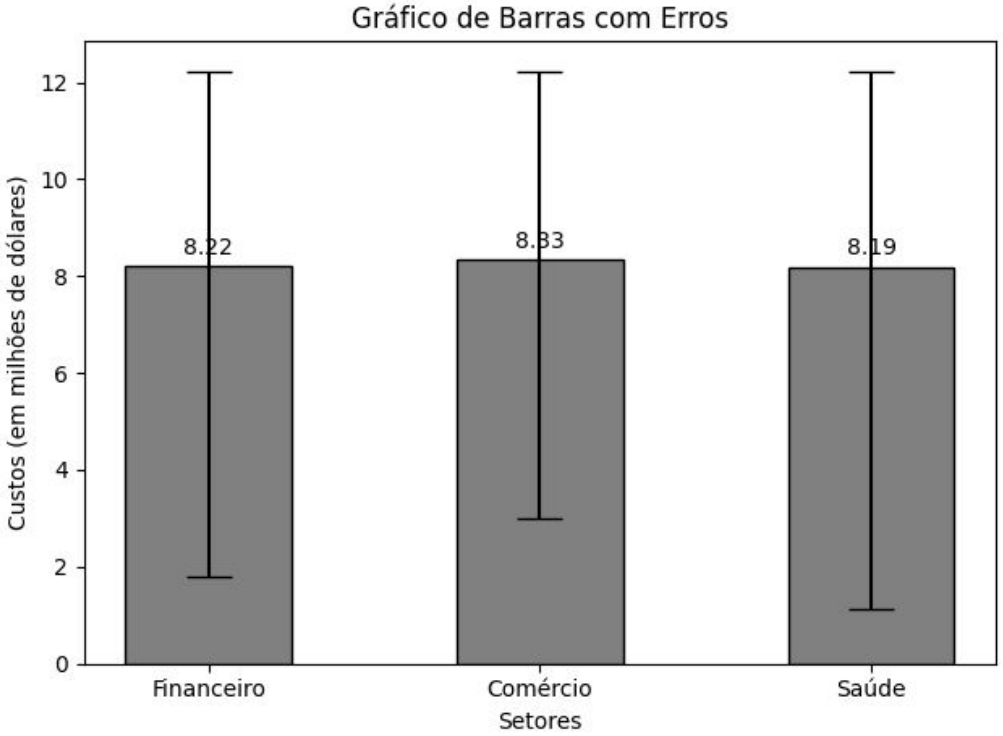


Simulações (2)

- Utilização das 315 requisições
    - 100 rodadas por requisição
- Tempo de execução ≈ 4,11 segundos por rodada
    - 36 horas para todas as 31500 rodadas
- Obtenção dos riscos e impactos financeiros
- Análise dos resultados
    - Por setor
    - Por tipo de ataque

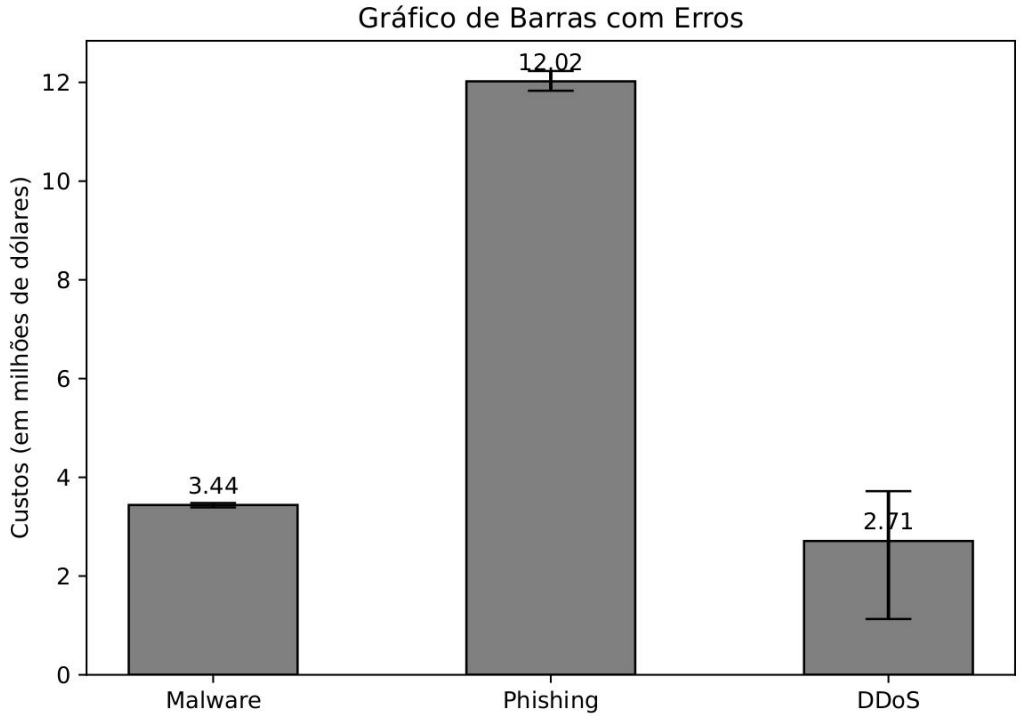
Simulações (3)

- Custos médios por setor



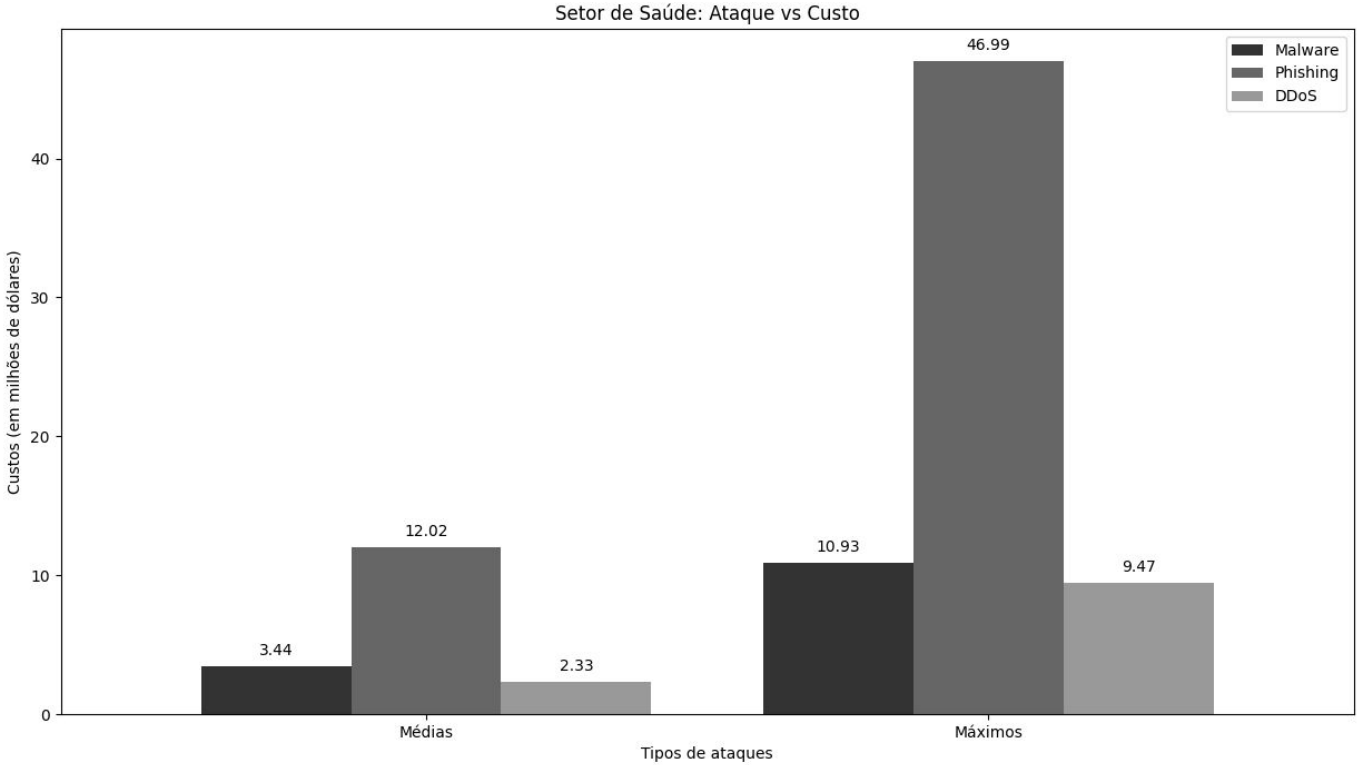
Simulações (4)

- Custos médios por tipo de ataque



Simulações (5)

- Estudo de caso: setor de saúde



Resultados

Ciberataque: impactos financeiros significativos

Phishing: tipo de ataque mais custoso à uma empresa

Setor de saúde: maior variação no valor do custo médio

Conclusão

- Solução apoiada em dados reais
    - Relatórios
    - Estatísticas
- Solução visada nos aspectos técnicos e econômicos de ciberataques
- Solução eficiente para os riscos e impactos de ciberataques
    - Quantificação
    - Simulação
    - Avaliação

Trabalhos Futuros

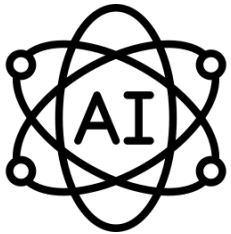
Metodologia

Relatório final

Coleta mais detalhada

Defesa vs Impactos

Plataforma interativa e cooperativa entre as empresas



IA para quantificação dos riscos e impactos

https://inf.ufrgs.br/gt-impacto

Obrigado!

SBSeg24
SÃO JOSÉ DOS CAMPOS

Perguntas?

jdmnunes@inf.ufrgs.br

.inf
INSTITUTO
DE INFORMÁTICA
UFRGS

Métricas

Métricas	Definição	Valores
Reputação	Classifica a EC em relação a sua reputação técnica e maturidade dos processos implementados	0= EC desconhecida 1= EC reconhecida nacionalmente 2= EC reconhecida mundialmente
Periodicidade	Verifica a frequência de publicações de dados da EC	0= Compilados de outras fontes 1= Publicação mensal/semestral 2= Publicação anual
Cobertura	Verifica o alcance do estudo dos relatórios publicados, em relação à um país/-continente ou globalmente	0= EC não menciona 1= Cobertura local/continental 2= Cobertura global
Escopo	Avalia se a EC publica relatórios com dados de um único ou de múltiplos setores da indústria	0= EC não menciona 1= Setorial (único) 2= Multisetorial
Abrangência dos ataques	Indica se a EC publica relatórios sobre um tipo de ciberataque ou mais	0= EC não menciona 1= Apenas um tipo de ataque 2= Tipos variados de ataques
Metodologia de pesquisa	Tem como foco analisar se a EC utilizou métodos bem definidos para a coleta e fornecimento dos dados	0= Sem metodologia 1= Sem metodologia mas com inferências 2= Possuem metodologias e apresentam resultados completos

Exemplos de ECs, Métricas e Notas

$$TP = \frac{(Rep*P_{Rep})+(Per*P_{Per})+(Cob*P_{Cob})+(Esc*P_{Esc})+(Abr*P_{Abr})+(Met*P_{Met})}{P_{Rep}+P_{Per}+P_{Cob}+P_{Esc}+P_{Abr}+P_{Met}} * 3$$

Pesos

Reputação	Periodicidade	Cobertura	Escopo	Abrangência	Metodologia
10	5	8	6	5	10

	Reputação *(Rep)*	**Periodicidade *(Per)***	**Cobertura *(Cob)***	**Escopo *(Esc)***	**Abrangência dos Ataques *(Abr)***	**Metodologia de Pesquisa *(Met)***	**Total com Peso *(TP)***	**Notas**
Radware	1	1	2	1	2	2	4.5	Relevante
Verizon	2	2	2	2	2	2	6	Muito Relevante
Zayo	1	1	1	1	1	1	3	Relevante

Trabalhos Relacionados

Solução	Objetivo	Relatórios Estatísticos	Simulações	Análise de Riscos	Impactos Econômicos
[Gordon et al. 2021]	Cálculo de investimento ótimo em cibersegurança	Não	Sim	Não	Sim
RCVaR (FRANCO et al., 2024)	Calcular as possíveis perdas financeiras em caso de ciberataques	Sim	Não	Não	Sim
(KIA et al., 2024)	Classificação e predição de riscos usando informações de CVEs e dados da Wikipedia	Não	Não	Sim	Não
(SUBROTO; APRIYANA, 2019)	Predição de riscos e vulnerabilidades usando dados de redes sociais	Não	Não	Sim	Não
SecRiskAI (FRANCO et al., 2022)	Análise de riscos de ciberataques em empresas usando IA	Não	Não	Sim	Não
EPSS (JACOBS et al., 2023)	Predição de riscos e priorização de vulnerabilidades usando EPSS	Sim	Sim	Sim	Não
SIM-Ciber (Este trabalho)	Classificação de relatórios, simulação de riscos e impactos econômicos	Sim	Sim	Sim	Sim