IMPACTO: Plataforma de Capacitação em Cibersegurança Baseada em Simulação de Aspectos Econômicos de Ciberataques

Laura R. Soares[1], **Muriel F. Franco**[2], **João M. Nunes**[1], **Henrique Lindemann**[1], **Geancarlo Kozenieski**[1], **Jéferson C. Nobre**[1]

[1]Universidade Federal do Rio Grande do Sul (UFRGS)
[2]Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)

{lrsoares, jdmnunes, hlindemann, gkozenieski, jcnobre}@inf.ufrgs.br, muriel.franco@ufcspa.edu.br

Abstract. *Cybersecurity planning represents a challenge for companies operating with limited technical and financial resources, especially in the face of the growth in cyberattacks and their economic impact. In this context, we developed IMPACTO to support training students and professionals in the field, focusing on risk analysis and investment planning in cybersecurity. The platform integrates technical and economic aspects through simulations based on realistic scenarios, using data from public reports and state-of-the-art economic models. The IMPACTO platform promotes applied and structured learning, allowing the user to understand the financial impact of different defense strategies and the risks in different contexts. Usability and functionality evaluations have been carried out, and the results indicate high effectiveness as an educational and decision-making support tool.*

Resumo. *O planejamento em cibersegurança representa um desafio para empresas que operam com recursos técnicos e financeiros limitados, especialmente diante do crescimento de ataques cibernéticos e de seus impactos econômicos. Nesse contexto, a plataforma IMPACTO foi desenvolvida para apoiar a formação de estudantes e profissionais da área, com foco na análise de riscos e no planejamento de investimentos em cibersegurança. A plataforma integra aspectos técnicos e econômicos por meio de simulações baseadas em cenários realistas, utilizando dados de relatórios públicos e modelos econômicos do estado da arte. A plataforma IMPACTO promove um aprendizado aplicado e estruturado, permitindo ao usuário compreender o impacto financeiro de diferentes estratégias de proteção, bem como os riscos em diferentes contextos. Avaliações de usabilidade e funcionalidade foram realizadas, e os resultados indicam uma alta eficácia como ferramenta educacional e de apoio à tomada de decisão.*

1. Introdução

Estima-se que o gasto global em Segurança da Informação poderá atingir até 212 bilhões de dólares em 2025 [Gartner 2024], movido por fatores como a adoção de ferramentas

de Inteligência Artificial Generativa (GenAI) e a migração contínua para serviços de infraestrutura em nuvem pública. Pequenas e Médias Empresas (PMEs) muitas vezes carecem de um planejamento efetivo de estratégias de cibersegurança sob o viés técnico e econômico [Franco et al. 2023]. Profissionais da área necessitam de ferramentas e abordagens que explorem os conceitos de economia e cibersegurança de forma integrada [Kianpour et al. 2021, Franco et al. 2024], permitindo assim um melhor planejamento e comunicação entre equipes técnicas e gestores durante o planejamento e investimento em cibersegurança [Fedele and Roner 2022].

A dimensão econômica é parte essencial de um planejamento de cibersegurança robusto, pois evita o desperdício de recursos em soluções que não contemplam as necessidades de uma organização [Gordon et al. 2020]. Porém, poucas soluções focam no treinamento de profissionais sob uma perspectiva econômica. Além disso, a maior parte das soluções existentes se concentra nas necessidades de grandes empresas com muitos recursos e ativos. Elas não abordam a fundo conceitos de modelos econômicos aplicados à cibersegurança, e também não possuem viés educacional. A plataforma IMPACTO é uma plataforma educacional para capacitação de profissionais de cibersegurança, utilizando relatórios da indústria e técnicas de simulação para guiar alunos e consultores de cibersegurança no processo de análise de impactos econômicos de ciberataques e no planejamento de estratégias eficientes.

A plataforma IMPACTO integra conceitos técnicos de cibersegurança e fundamentos de economia, oferecendo experiências práticas que desenvolvem competências analíticas em identificação de ameaças, avaliação de riscos, definição de estratégias de proteção e análise de investimentos em segurança. Em ambientes educacionais, os estudantes seguem um fluxo de aprendizado estruturado, aplicando conhecimentos de cibersegurança e modelos econômicos para resolver problemas reais. Essa abordagem estimula o desenvolvimento de habilidades críticas e a compreensão integrada dos desafios do setor, preparando os alunos para atuar de forma estratégica em diferentes contextos profissionais.

O desenvolvimento da plataforma IMPACTO ocorreu no contexto do Programa Hackers do Bem[1], da Rede Nacional de Ensino e Pesquisa (RNP). Assim, as funcionalidades da plataforma tem como foco a capacitação em cibersegurança para os alunos do programa, estudantes de áreas correlatas e também profissionais da área. A plataforma IMPACTO foi avaliada junto aos alunos de residência tecnológica do programa Hackers do Bem, comprovando a aplicabilidade dos conceitos abordados junto à nova geração de profissionais de cibersegurança. A versão inicial da plataforma está disponível publicamente para acesso em `https://gt-impacto.inf.ufrgs.br/`.

O restante deste artigo está organizado do seguinte modo. A Seção 2 apresenta a plataforma IMPACTO, incluindo a arquitetura e principais funcionalidades. Na Seção 3 é apresentada a avaliação junto aos usuários do programa Hackers do Bem e demais públicos-alvo da plataforma. Nesta seção também são apresentados os principais resultados da avaliação em relação à funcionalidade e usabilidade da plataforma. Por fim, na Seção 4, são apresentadas as considerações finais e trabalhos futuros.

[1]https://hackersdobem.org.br/formacao

2. Plataforma IMPACTO

A plataforma IMPACTO tem como foco o ensino de cibersegurança para capacitação de consultores e profissionais da área. Instrutores de cursos de Segurança da Informação podem, por exemplo, usar a ferramenta para elaborar cenários de estudo hipotéticos ou baseados em empresas reais. Tais cenários são então usados por alunos para a realização de exercícios e simulações de análise de risco e planejamento econômico. A arquitetura do IMPACTO é apresentada na Figura 1, estruturada de modo a apresentar as principais etapas durante o uso da plataforma.

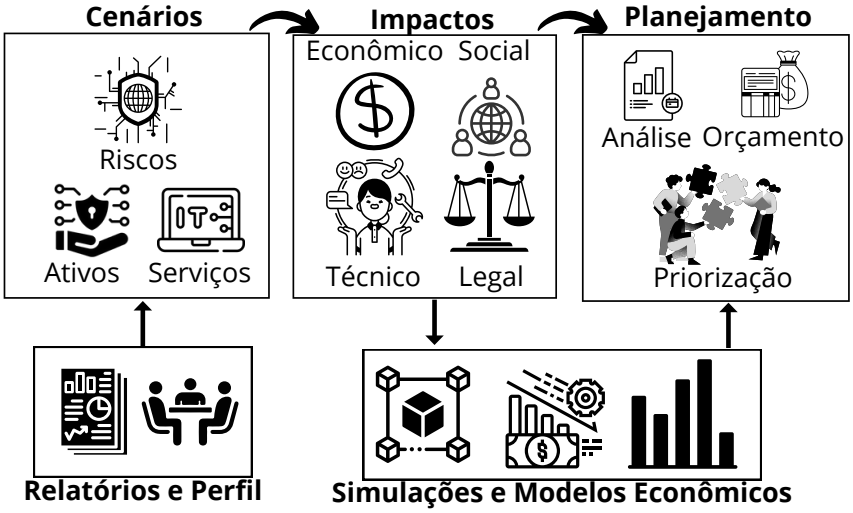

Figura 1. Arquitetura da plataforma IMPACTO.

A arquitetura da plataforma foi planejada em um modelo de pipeline, onde a saída de um módulo é usada como entrada para o módulo seguinte. Primeiro, relatórios da indústria sobre ciberataques foram coletados e modelados em um banco de dados. Durante o uso da ferramenta, as informações no banco de dados são usadas em conjunto com o cenário de estudo, preparado por um instrutor, com as características da empresa hipotética que servirá como objeto da análise. Esses dois módulos alimentam a ferramenta de análise de riscos, que se baseia em informações como a área de atuação da empresa e sua estrutura de cibersegurança existente. A pontuação de risco calculada nesse módulo é usada pelo módulo de gestão econômica, que aplica modelos econômicos do estado da arte para avaliar o investimento ótimo em cibersegurança correspondente aos ativos do cenário.

Durante a interação com a plataforma, alunos e instrutores realizam alterações nos detalhes do cenário e estudam como as mudanças impactam tanto na vulnerabilidade da empresa hipotética quanto na eficiência dos investimentos em soluções de cibersegurança. Uma demonstração da plataforma está disponível publicamente em `https://www.youtube.com/watch?v=x0RAgu_bjSU`.

2.1. Base de Dados de Relatórios da Indústria

A base de dados da plataforma recebe como entrada informações de relatórios de cibersegurança de empresas conhecidas no ramo, tais como os relatórios disponíveis em [IBM 2024] e [Verizon 2025]. Essas empresas coletam diversas informações sobre

o funcionamento de organizações parceiras, incluindo dados técnicos sobre incidentes de segurança, valores de perdas monetárias, ameaças emergentes, entre outras. Esses dados são modelados conforme o setor de atuação da empresa, sua localização, e o tipo de ciberataque sofrido, para então serem armazenados na base de dados da plataforma IMPACTO. A lista com exemplos dos relatórios usados na plataforma está disponível no Apêndice A.

2.2. Módulo de Análise de Riscos

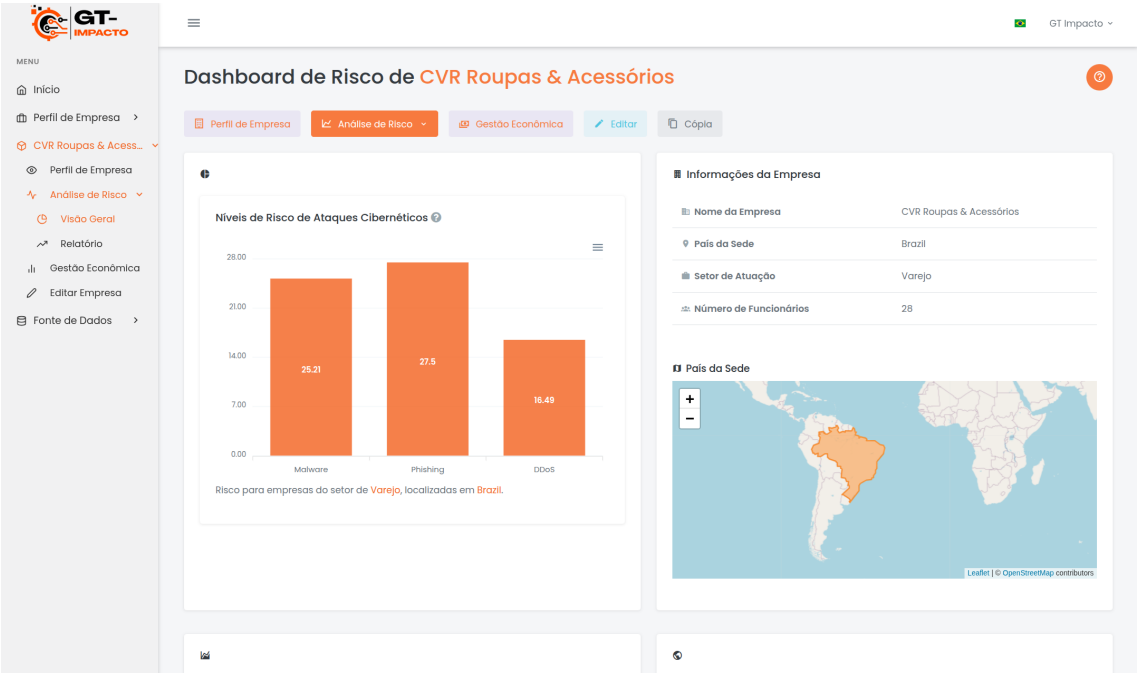

Figura 2. Captura de tela do módulo de Análise de Riscos, na aba *Visão Geral*.

O Módulo de Análise de Riscos da plataforma IMPACTO é dividido em duas abas: *Visão Geral* e *Relatório*. A aba *Visão Geral* aparece na Figura 2. Nela, os dados coletados dos relatórios são usados para apontar a probabilidade da empresa usada como cenário de estudo sofrer ataques de *malware*, *phishing* e DDoS. Essa probabilidade é calculada com base no setor da indústria em que a empresa atua e em sua localização. A aba *Visão Geral* também traz as informações relevantes sobre o perfil da empresa e um panorama de riscos geral do setor e da região. Durante o uso da plataforma, alunos podem usar essas informações para fazer inferências sobre o cenário de estudo com a ajuda de um instrutor.

Na aba *Relatório* (Figura 3), as probabilidades de ataque calculadas previamente são integradas com dados técnicos da empresa para oferecer uma análise quantitativa de risco. Com esses dados, a plataforma calcula uma Pontuação de Risco (PR) [Nunes et al. 2024] baseando-se em três variáveis: setor, região e resiliência. Para o cálculo de risco da região e do setor, as probabilidades condicionais de ataque são extraídas do banco de dados ($P_{ataque|setor}$, $P_{ataque|pais}$, $P_{ataque|continente}$) para cada tipo de ciberataque (*malware*, *phishing* e DDoS). Calcula-se a média (M) e o desvio padrão (DP), e, conforme a posição relativa da empresa nessas distribuições, atribui-se um peso entre 0,3 e 2,0, refletindo seu risco setorial e regional. Esses cálculos estão detalhados na Tabela 1.

Quanto menor a probabilidade de ataque na empresa, menor é o risco apresentado e menor é o valor refletido na PR. A preparação da empresa é determinada por suas medidas de cibersegurança e por seu histórico de ataques. São então atribuídos pesos às informações obtidas, sob o ponto de vista da eficácia contra o ciberataque (impactantes, relevantes ou indiferentes), conforme a Tabela 4 no Apêndice A. O valor final de preparação varia entre 0,5 e 4,5, sendo utilizado como fator de penalização inversa no cálculo do risco.

Ao coletar todas as informações, o cálculo da pontuação de risco da empresa para aquele ciberataque é então realizado conforme as equações da Tabela 1, com o valor base sendo 6. A média simples entre os três valores é usada para fornecer uma pontuação geral da empresa. A aba também apresenta o impacto de cada controle de segurança sobre os pilares de confidencialidade, integridade e disponibilidade. A plataforma permite que os alunos modifiquem os controles adotados pela empresa-cenário e observem, em tempo real, os efeitos dessas mudanças nas pontuações de risco.

Tabela 1. Fórmulas da Pontuação de Risco

ValorBase	6
Risco do Setor	$Risco_{setor}$ = Pior Risco do Setor $\longrightarrow Valor = 0.3$ $Risco_{setor} \leq$ M+DP $\longrightarrow Valor = 0.5$ M-DP $\leq Risco_{setor} \leq$ M+DP $\longrightarrow Valor = 0.8$ $Risco_{setor} \geq$ M+DP $\longrightarrow Valor = 1.25$ $Risco_{setor}$ = Maior Risco do Setor $\longrightarrow Valor = 2.0$
Risco do País	Similar ao Risco do Setor
Risco do Continente	Similar ao Risco do Setor
Risco da Região	$\frac{Valor_{pais} \times Valor_{continente}}{2}$
Resiliência	$\frac{1}{Preparacao}$
Pontuação de Risco (por ciberataque)	$\min\left(ValorBase \times Risco_{regiao} \times Risco_{setor} \times Resiliencia,\ 10\right)$
Pontuação de Risco Geral	$\frac{\sum PR_{ciberataques}}{\sum Ciberataques}$

2.3. Módulo de Planejamento Econômico

A página de gestão econômica usa a pontuação de risco calculada para o cenário de estudo no módulo anterior, combinada com as informações financeiras da empresa. Essas informações são o valor dos ativos da empresa em risco e os investimentos atuais em soluções de cibersegurança. Com esses dados, a plataforma fornece ao usuário uma orientação didática sobre o valor ótimo de investimento em medidas protetivas para o cenário.

O modelo de Gordon-Loeb [Gordon et al. 2020] é utilizado para o cálculo do investimento ótimo no módulo de gestão econômica. Ele fornece uma estimativa dos impactos econômicos de um ciberataque e ajuda a otimizar os investimentos em cibersegurança para proteger um ativo da empresa. O modelo propõe que, considerando a vulnerabilidade de um sistema e a potencial perda financeira causada por um ciberataque, a companhia direcione sua estratégia de investimentos em sistemas de segurança que diminua o prejuízo esperado sem investimentos desnecessários. A equação utilizada para calcular o EBIS (*Expected Benefit of Information Security*, ou benefício esperado da segurança da informação) de cada ativo leva em conta a vulnerabilidade do sistema, calculada no

Figura 3. Captura de tela do módulo de Análise de Riscos, na aba *Relatório*.

módulo de análise de risco, e o potencial de perda por um ciberataque, além do valor investido. Através dessa modelagem, é possível encontrar o valor de investimento com melhor rendimento, ou seja, que apresenta o maior ENBIS (*Expected Net Benefit of Information Security*, ou benefício líquido esperado) considerando o custo do investimento.

A página de Gestão Econômica é dividida em duas partes, conforme apresentado na Figura 4. Primeiro, uma tabela fornece uma análise da eficiência do investimento e quais ajustes são necessários para alcançar o ENBIS máximo para cada tipo de ataque. A segunda parte da página apresenta o gráfico do EBIS em função do valor de investimento, aponta os valores atuais e ótimos de investimento e verifica se o investimento atual está dentro do intervalo aceitável. Alunos e instrutores podem fazer alterações nos parâmetros de simulação, permitindo comparar quais ferramentas de cibersegurança mais se aproximam dos valores ótimos de investimento para o cenário.

3. Avaliação

A plataforma IMPACTO foi avaliada por alunos do Programa Hackers do Bem e também por alunos de graduação e pós-graduação em áreas correlatas à cibersegurança. No total, tivemos 28 participantes na avaliação com idade entre 20 e 40 anos. Durante a avaliação, foi realizada uma avaliação para determinar se as principais funcionalidades da plataforma auxiliam os participantes na resolução de atividades referentes ao planejamento e análise econômica de cibersegurança. Além disso, a plataforma passou por uma avaliação de usabilidade com os mesmos participantes utilizando o método System Usability Score (SUS).

3.1. Casos de Uso e Demonstração

A avaliação da plataforma utilizou uma sequência estruturada de atividades, embora esse fluxo não seja obrigatório para o uso geral. O processo de avaliação consiste no uso da

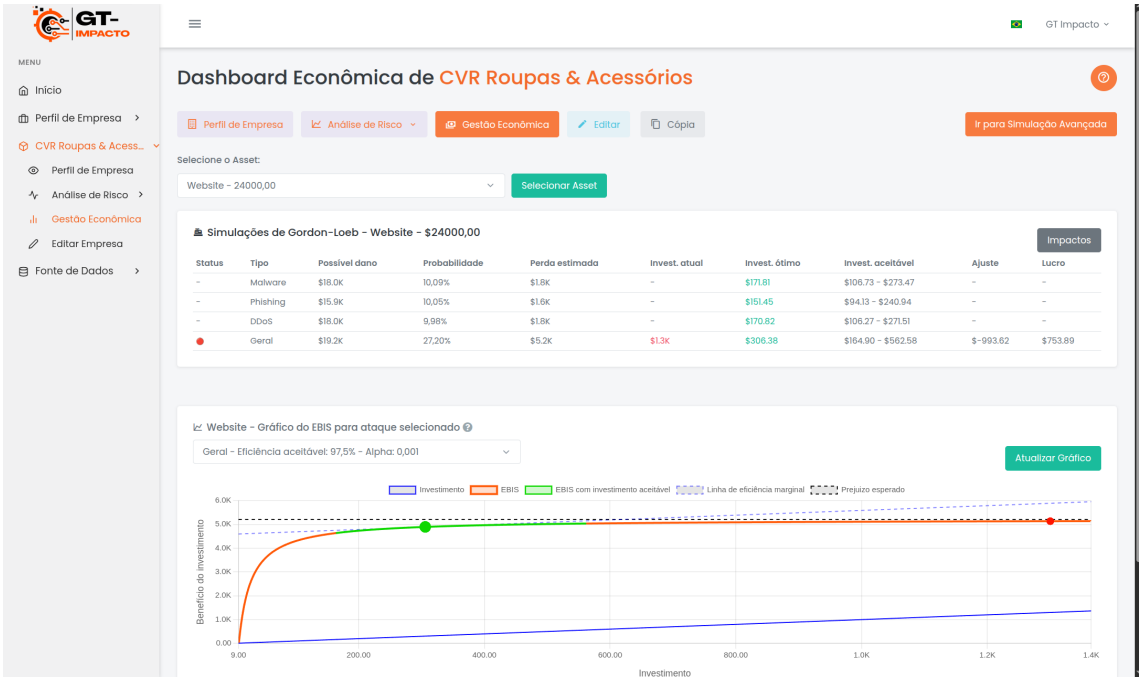

Figura 4. Captura de tela da página de Planejamento Econômico.

plataforma da seguinte maneira: (*i*) identificação do ataque cibernético de maior risco na página *Visão Geral*; (*ii*) consulta à página *Relatório* para determinar o nível de resiliência da empresa; (*iii*) simulações práticas com criação de cópias do cenário e modificação de medidas de cibersegurança; (*iv*) análise econômica e verificação no módulo de Gestão Econômica se o investimento atual corresponde ao valor ótimo calculado pelo modelo Gordon-Loeb; e (*v*) exploração da área *Fonte de Dados* para identificar setores sob maior risco de ataques específicos.

3.2. Resultados

A avaliação da plataforma IMPACTO foi conduzida com 28 participantes, sendo 20 deles (71,4%) provenientes do programa Hackers do Bem e 8 (28,6%) de outras origens, principalmente vinculados a instituições de ensino superior. A metodologia de avaliação foi estruturada em quatro etapas sequenciais: preparação com formulário de consentimento e coleta de dados demográficos, avaliação de funcionalidade por meio de exercícios práticos, avaliação de usabilidade utilizando o questionário SUS. Além disso, devido à sua natureza educacional, também foi realizada uma avaliação de adequação curricular específica para participantes do programa Hackers do Bem.

Os exercícios de funcionalidade abordaram diferentes aspectos da plataforma, desde navegação até análise econômica avançada. A Tabela 2 apresenta exemplos de atividades realizadas e as taxas de acerto obtidas em cada exercício, demonstrando a eficácia da plataforma como ferramenta de ensino. A média geral de acertos foi de 93,45%. As funcionalidades básicas de visualização e análise apresentaram excelente desempenho. Por outro lado, funcionalidades mais complexas, como o mecanismo de cópias de cenários e a especificação precisa de valores monetários, evidenciaram oportunidades de aprimoramento para o contexto educacional.

Além disso, o questionário SUS para avaliação de usabilidade resultou em uma

Tabela 2. Exercícios realizados e taxa de acertos por exercício na avaliação de funcionalidade

Exercício		Acertos	Taxa
1	Identificação de ataque de maior risco	28	100%
2	Verificação do nível de resiliência da empresa	27	96,43%
3	Simulação com alterações de cenário e cópias de empresa	25	89,29%
4.1	Verificação de investimento ótimo	27	96,43%
4.2	Valor específico do investimento ótimo	23	82,14%
5	Identificação de setor com maior risco DDoS	27	96,43%

pontuação média de 85,28, considerada excelente e equivalente à nota A+ na escala de usabilidade. Esta pontuação indica alta usabilidade da plataforma, facilidade de interação, satisfação dos usuários e interface intuitiva. O resultado está no limite superior de excelência (80+ pontos), validando a adequação da ferramenta para uso em ambientes de ensino. Já a avaliação de adequação curricular indicou que os participantes consideraram o conteúdo da plataforma relevante e alinhado à sua formação em cibersegurança e modelos econômicos. O *feedback* qualitativo foi amplamente positivo, destacando a interface intuitiva e a utilidade dos recursos para o aprendizado, além de apontar sugestões construtivas para aprimoramento.

A avaliação com usuários do público-alvo da plataforma IMPACTO permitiu não só a validação das funcionalidades desenvolvidas até o momento como também o mapeamento de melhorias para futuras versões. O *feedback* fornecido pelos participantes indicou a necessidade de modificações em algumas das interfaces. Por exemplo, no módulo de gestão econômica, as informações precisam ser compartimentalizadas de modo a tornar a experiência menos complexa para os usuários. Outras sugestões de melhorias obtidas durante a avaliação são referentes a funcionalidades complementares, como a possibilidade de comparação entre os cenários de estudo antes e depois das modificações feitas pelos alunos.

4. Considerações Finais

A plataforma IMPACTO busca suprir a necessidade de soluções que possibilitem a compreensão de aspectos econômicos de ciberataques, análise de riscos e o planejamento de investimentos em cibersegurança. Sua característica principal é o foco na capacitação de profissionais através do uso de cenários de treinamento, mostrando de forma clara e educacional os modelos e conceitos usados nas análises. A estrutura modular da plataforma permite adaptação a diferentes contextos educacionais, desde introduções básicas até análises avançadas de planejamento econômico. A avaliação de usabilidade demonstrou alto índice de sucesso na execução das tarefas propostas, confirmando o potencial da ferramenta para o desenvolvimento de competências analíticas em cibersegurança e modelos econômicos.

Como trabalhos futuros, será desenvolvido um módulo para a recomendação de proteções baseadas em orçamento definido e também integração com métricas técnicas para priorização de riscos, como, por exemplo, o Exploit Prediction Scoring System (EPSS). Além disso, diferentes cenários serão definidos para a capacitação de profissionais de cibersegurança que atuam em setores críticos (por exemplo, Saúde

[Franco et al. 2025] e Financeiro [Gulyas and Kiss 2023]) e que necessitam de eficiência econômica durante o planejamento em cibersegurança.

Referências

Fedele, A. and Roner, C. (2022). Dangerous Games: A Literature Review on Cybersecurity Investments. *Journal of Economic Surveys*, 36(1):157–187.

Franco, M., Omlin, C., Kamer, O., Scheid, E., Granville, L., and Stiller, B. (2024). SECAdvisor: A Tool for Cybersecurity Planning using Economic Models. In *XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 554–569, São José dos Campos/SP.

Franco, M. F., Granville, L. Z., and Stiller, B. (2023). CyberTEA: A Technical and Economic Approach for Cybersecurity Planning and Investment. In *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pages 1–6. IEEE.

Franco, M. F., Soares, L. R., and Nobre, J. C. (2025). Saúde Sob Ataque: Da Avaliação de Riscos ao Desenvolvimento de Estratégias de Investimentos em Cibersegurança na Área da Saúde. *XXV Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2025)*, 36:1–44.

Gartner (2024). Gartner Forecasts Global Information Security Spending to Grow 15 `https://shorturl.at/Z2FVb`. Acessado em julho de 2025.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2020). Information segmentation and investing in cybersecurity. *Journal of Information Security*, 12(1):115–136.

Gulyas, O. and Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, 219:84–90.

IBM (2024). X-Force Threat Intelligence Index 2024. `https://shorturl.at/yaZ4G`. Acessado em julho de 2025.

Kianpour, M., Kowalski, S. J., and Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability*, 13(24):13677.

Nunes, J., Franco, M., Scheid, E., Kozenieski, G., Lindemann, H., Soares, L., Nobre, J., and Granville, L. (2024). Sim-ciber: Uma solução baseada em simulações probabilísticas para quantificação de riscos e impactos de ciberataques utilizando relatórios estatísticos. In *XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 570–585.

Verizon (2025). Data Breach Investigations Report (DBIR). `https://shorturl.at/amkeZ`. Acessado em julho de 2025.

Apêndice A

Tabela 3. Exemplos de Relatórios Utilizados como Fontes de Dados

Nome	Organização
Acronis Mid-Year Cyberthreats Report 2023	Acronis
DDoS Threat Landscape Report 2023	Arelion
Blackpoint Cyber Annual Threat Report 2024	Blackpoint
Healthcare Industry Was the Most Common Victim of Third-Party Breaches in 2022	Black Kite
Checkpoint Cybersecurity Report 2024	Check Point Software
Deepwatch Annual Threat Report 2024	Deepwatch
ENISA Threat Landscape 2024	ENISA
Ensign Cyber Threat Landscape Report 2024	Ensign InfoSecurity
Expel Annual Threat Report 2024	Expel
Flashpoint Midyear CTI Index 2024	Flashpoint
Retail Cybersecurity Statistics Not To Be Ignored	Fortinet
Guidepoint Ransomware Annual Report 2024	GuidePoint Security
IBM X-Force Threat Intelligence Index 2024	IBM
M-Trends 2024 Special Report	Mandiant
2022 in review: DDoS attack trends and insights	Microsoft
Microsoft Digital Defense Report 2024	Microsoft
2023 State of the Phish	Proofpoint
2022 Global Threat Analysis Report	Radware
The State of Ransomware in Financial Services 2023	Sophos
2022: DDoS Year-in-Review Report by StormWall	Stormwall
2024 Data Breach Investigations Report	Verizon
WatchGuard Threat Report 2024	WatchGuard
Zscaler ThreatLabz 2024 Ransomware Report 2024	Zscaler

Tabela 4. Exemplo de Classificação das Medidas de Segurança por Ciberataque

Item	MALWARE	PHISHING	DDOS
Inventário Atualizado	Relevante	Relevante	Relevante
Manutenção de Backup	Impactante	Indiferente	Indiferente
Priorização de Riscos	Relevante	Relevante	Relevante
Fatores de Autenticação	Impactante	Impactante	Indiferente
Tipo de Solução de Nuvem	Indiferente	Indiferente	Impactante
Atualização Periódicas de Sistema	Impactante	Relevante	Relevante
VPN para Acesso Remoto	Negativa	Negativa	Indiferente