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 poses a challenge for resource-constrained companies, particularly given the rise in cyberattacks and their economic consequences. IMPACTO is an innovative solution designed to train students and professionals in cybersecurity economics, with a special focus on Small and Medium-sized Enterprises (SMEs). Developed to support the training of students and professionals, the platform combines risk analysis with cybersecurity investment planning, integrating technical and economic aspects through realistic scenario simulations based on public report data and advanced economic models. The tool facilitates the study and formulation of security strategies, enabling managers and technical staff to understand the financial impact of attacks and technical decisions. IMPACTO offers hands-on learning, helping users grasp the financial implications of various protection strategies and risks across different contexts. Usability and functionality assessments have demonstrated its high effectiveness as an educational tool and an aid to decision-making.*

Resumo. *O planejamento em cibersegurança é um desafio para empresas com recursos limitados, principalmente diante do aumento dos ataques cibernéticos e de suas consequências econômicas. A IMPACTO é uma solução inovadora para capacitar alunos e profissionais nos conceitos de economia da cibersegurança, com atenção especial às Pequenas e Médias Empresas (PMEs). Desenvolvida para apoiar a formação de estudantes e profissionais, a plataforma une análise de riscos e planejamento de investimentos em cibersegurança, integrando aspectos técnicos e econômicos por meio de simulações de cenários realistas, com dados de relatórios públicos e modelos econômicos avançados. A ferramenta possibilita o estudo e a elaboração de estratégias de segurança, permitindo que gestores e técnicos compreendam os impactos financeiros de ataques e de decisões técnicas. A IMPACTO oferece aprendizado prático, ajudando o usuário a entender o efeito financeiro de diferentes estratégias de proteção e os riscos em diversos contextos. Avaliações de usabilidade e funcionalidade demonstraram sua alta eficácia como ferramenta educacional e apoio à tomada de decisão.*

1. Introdução

O investimento global em Segurança da Informação poderá atingir 212 bilhões de dólares em 2025 [Gartner 2024], impulsionado pela adoção de ferramentas de Inteligência Artificial Generativa (GenAI) e pela migração contínua para serviços de infraestrutura em nuvem pública. Nesse contexto, Pequenas e Médias Empresas (PMEs) frequentemente apresentam lacunas no planejamento de estratégias de cibersegurança sob as perspectivas técnica e econômica [Franco et al. 2023]. Como resultado, profissionais do setor demandam ferramentas e abordagens que integrem conceitos de economia e de cibersegurança [Kianpour et al. 2021, Franco et al. 2024], promovendo o alinhamento entre equipes técnicas e gestores no processo decisório sobre investimentos em cibersegurança [Fedele and Roner 2022].

A dimensão econômica é essencial para o planejamento eficaz de cibersegurança, pois evita o desperdício de recursos em soluções inadequadas às necessidades organizacionais [Gordon et al. 2020]. No entanto, poucas soluções priorizam o treinamento de profissionais sob a perspectiva econômica. Além disso, a maioria das soluções existentes é voltada principalmente a grandes empresas com recursos e ativos significativos, sem abordar de forma aprofundada os modelos econômicos aplicados à cibersegurança nem oferecer um enfoque educacional. Nesse cenário, a plataforma IMPACTO destaca-se como uma solução educacional voltada à capacitação de profissionais de cibersegurança, utilizando relatórios da indústria e técnicas de simulação para orientar alunos e consultores na análise dos impactos econômicos de ciberataques e no planejamento de estratégias eficazes.

A plataforma IMPACTO integra conceitos técnicos de cibersegurança e fundamentos econômicos, proporcionando experiências práticas que desenvolvem competências analíticas para a identificação de ameaças, a avaliação de riscos, a definição de estratégias de proteção e a análise de investimentos em segurança. Durante esse processo, os estudantes seguem um percurso de aprendizado estruturado, aplicando conhecimentos de cibersegurança e de modelos econômicos na resolução de problemas reais. Essa abordagem favorece o desenvolvimento de habilidades críticas e a compreensão integrada dos desafios do setor, preparando os alunos para atuação estratégica em diferentes contextos profissionais.

O desenvolvimento da plataforma IMPACTO ocorreu no âmbito do Programa Hackers do Bem[1], da Rede Nacional de Ensino e Pesquisa (RNP). Assim, as funcionalidades da plataforma são voltadas à capacitação em cibersegurança de alunos do programa, de estudantes de áreas correlatas e de profissionais do setor. A plataforma IMPACTO foi avaliada por alunos de residência tecnológica do programa Hackers do Bem, o que demonstrou a aplicabilidade dos conceitos à nova geração de profissionais de cibersegurança. A versão inicial da plataforma está disponível em um repositório público em `https://github.com/ComputerNetworks-UFRGS/IMPACTO-Demo`.

O restante deste artigo está organizado do seguinte modo. Primeiro, a Seção 2 mostra um comparativo de soluções relacionadas à proposta da plataforma IMPACTO. A Seção 3 apresenta a plataforma IMPACTO, incluindo a arquitetura e principais funcionalidades. Na Seção 4 é apresentada a avaliação junto aos usuários do programa Hackers

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

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 5, são apresentadas as considerações finais e trabalhos futuros.

2. Soluções Relacionadas

Empresas são cada vez mais dependentes do meio digital, seja para prestar seus serviços, seja para utilizar ferramentas adjacentes ao processo produtivo. Esse fato leva diretamente ao aumento do número de ciberataques, que, por sua vez, resulta em um crescimento significativo do mercado de soluções de gerenciamento de cibersegurança [Aiyer et al. 2022]. É evidente que esse setor ainda é amplamente dominado por soluções robustas, porém caras e complexas, geralmente projetadas para atender às demandas de grandes empresas [European Commission 2020]. É comum que uma PME tenha restrições na disponibilidade de recursos e de pessoal com experiência técnica em cibersegurança [Franco et al. 2023], o que pode ser um impedimento para adquirir e configurar as várias ferramentas que compõem uma estratégia de segurança global e robusta.

O mapeamento das principais soluções do mercado para gerenciamento de cibersegurança é apresentado na Tabela 1. Foram comparadas soluções para automatizar as análises de risco e a avaliação da segurança da estrutura existente. É possível perceber que a maioria das soluções disponíveis tem origem em empresas dos EUA, o que evidencia a centralização do mercado e a falta de soluções adaptadas a cenários e necessidades locais. Além disso, os custos elevados dificultam o acesso das PMEs ao mercado, visto que, além do custo da licença, há custos de operação, como o treinamento de pessoal e a compra de equipamentos específicos. Finalmente, as ferramentas observadas, em sua maioria, disponibilizam indicadores técnicos, sem focar em análises econômicas de ciberataques ou no planejamento de investimentos em cibersegurança.

Tabela 1. Mapeamento de Soluções do Mercado para Gerenciamento de Cibersegurança

Solução	Tipo	Natureza	País	Custo (anual)	Principais Técnicas
GT-IMPACTO	Análise de Riscos, Planejamento de Investimentos	Academia	Brasil	Free, Open-source	Análise de Riscos, Simulação de Investimentos
SECAdvisor [Franco et al. 2024]	Análise de Riscos, Planejamento de Investimentos	Academia	Suíça	Free, Open-source	Simulação de Investimentos, Recomendação de proteções
ZERON Cyber Risk Posture Management[2]	Gerenciamento de Riscos	Comercial	India	US$ 6,000 (Startups)	Análise automatizada de riscos e escaneamento de assets
AttackIQ[3]	Gerenciamento de Vulnerabilidades, Teste de Segurança	Comercial	EUA	US$ 5,000 (por cada Test Point Engine)	*Breach Attack Simulator*
Qualys VMDR[4]	Gerenciamento de Vulnerabilidades	Comercial	EUA	US$ 9000 (256 hosts)	Descoberta de ativos, varredura automatizada de vulnerabilidades. Priorização de ameaças
CyCognito Attack Surface Management Platform[5]	Gerenciamento de Assets e Vulnerabilidades	Comercial	EUA	US$ 30,000 (256 assets)	Teste automatizado de vulnerabilidades, descoberta de ativos
Utilis CCS[6]	Treinamento, Resposta a incidentes	Comercial	Croácia	Não disponível	Simulação de ataques para verificação de resposta a incidentes. Participação de diferentes stakeholders
Tanium[7]	Gerenciamento de Endpoints e Riscos	Comercial	EUA	US$ 36,000	Identifica vulnerabilidades em tempo real, prioriza e remedia os riscos.
ATTACK Simulator[8]	Treinamento de conscientização, Phishing	Comercial	Romênia	Não disponível	Execução de ataques simulados como forma de treinamento e conscientização

[2]https://www.zeron.one/

[3]https://www.attackiq.com/

[4]https://www.qualys.com/apps/vulnerability-management-detection-response/

As soluções do mercado foram também comparadas em relação à utilização de simulações para inferir dados ou comportamentos, conforme apresentado na Tabela 2. Apenas 3 das 9 soluções fazem uso de técnicas de simulação. Já os aspectos econômicos são negligenciados pela maioria das soluções e são considerados principalmente por soluções da academia e startups. Isso mostra o potencial de inovação de soluções que foquem na dimensão financeira, ao mesmo tempo alertando sobre riscos de ataques e vulnerabilidades. Além disso, existe uma carência de soluções que auxiliem no treinamento de consultores e profissionais de cibersegurança e que possuam capacidade para uso educacional. Por fim, frameworks e padronizações como o MITRE ATT&CK, NIST CSF e ISO 27000 possuem relevância para as soluções de mercado, já que permitem uma análise padronizada de diferentes aspectos técnicos da cibersegurança.

Tabela 2. Comparação entre Soluções do Mercado para Gerenciamento de Cibersegurança.

Solução	Simulação	Aspectos Econômicos	Uso Educacional	Planejamento Integrado	Modelos e Integrações
GT-IMPACTO	Sim	Sim	Sim	Parcial	Gordon-Loeb
SECAdvisor	Parcialmente	Sim	Sim	Parcial	Gordon-Loeb e ROSI
ZERON Cyber Risk Posture Management	Não	Sim	Não	Parcial	MITRE ATT&CK, CVaR, ROSI e Modelo Proprietário
AttackIQ	Sim	Não	Não	Não	MITRE ATT&CK
Qualys VMDR	Não	Não	Não	Parcial	CVE, CVSS e Modelos Proprietários
CyCognito Attack Surface Management Platform	Não	Não	Não	Parcial	MITRE ATT&CK Framework, NIST CSF, CIS e ISO/IEC 27000, e padrões de regulação e *compliance*
Utilis CCS	Sim	Não	Sim	Parcial	Não disponível
Tanium	Não	Não	Não	Parcial	Integração com Microsoft Sentinel
ATTACK Simulator	Sim	Não	Sim	Não	Integração com Active Directory

Baseado na análise apresentada, é possível perceber que o nicho de mercado explorado pela plataforma IMPACTO tem grande potencial para crescimento e expansão. A ferramenta IMPACTO permite compreender e aplicar conceitos de economia da cibersegurança por consultores e alunos, além de integrar modelos econômicos e conceitos técnicos durante o ciclo de planejamento de estratégias de cibersegurança. A integração de técnicas educacionais para tomada de decisões e planejamento de investimentos tem potencial de trazer benefícios tanto para pessoas em nível de gerência quanto para consultores em treinamento.

3. Plataforma IMPACTO

A plataforma IMPACTO é dedicada ao ensino de cibersegurança, visando capacitar consultores e profissionais do setor. Instrutores de cursos de Segurança da Informação podem utilizar a ferramenta para criar cenários de estudo, sejam hipotéticos ou baseados em organizações reais. Esses cenários são empregados por alunos em exercícios e simulações de análise de risco e planejamento econômico.

O instrutor começa detalhando o perfil de uma empresa hipotética, usando a aba ”Adicionar Perfil de Empresa”(acesso restrito a administradores). As informações do cenário são organizadas em três dimensões: Negócios (dados básicos como setor, localização e porte), Técnica (infraestrutura de segurança, como backups e uso de VPN), e Econômica (histórico de investimentos e dados financeiros relevantes). Também é

[5]https://www.cycognito.com/platform/attack-surface-management.php
[6]https://ccs.utilis.biz/
[7]https://www.tanium.com/
[8]https://attacksimulator.com/

possível adicionar um histórico de ataques para enriquecer a análise de riscos. O perfil criado fica disponível aos alunos, que têm acesso restrito e podem utilizar roteiros de exercícios para explorar os módulos de Análise de Riscos e Planejamento Econômico. Os alunos podem modificar características do cenário e observar o impacto dessas mudanças na vulnerabilidade e na eficiência dos investimentos em cibersegurança. Alterações podem ser salvas em Perfis "Cópia", exclusivos de cada aluno, facilitando a revisão e correção posterior dos exercícios.

A arquitetura do IMPACTO está ilustrada na Figura 1, organizada para apresentar as principais etapas de utilização da plataforma. A arquitetura da plataforma segue um modelo de pipeline, em que a saída de cada módulo serve como entrada para o próximo. Inicialmente, relatórios da indústria sobre ciberataques são coletados e organizados em um banco de dados. No uso da ferramenta, esses dados são combinados ao cenário de estudo preparado pelo instrutor, detalhando as características da empresa hipotética analisada. Ambos os módulos abastecem a ferramenta de análise de riscos, que considera fatores como o setor de atuação e a infraestrutura de cibersegurança da empresa. A pontuação de risco gerada alimenta o módulo de gestão econômica, que utiliza modelos econômicos avançados para determinar o investimento ideal em cibersegurança, de acordo com os ativos do cenário.

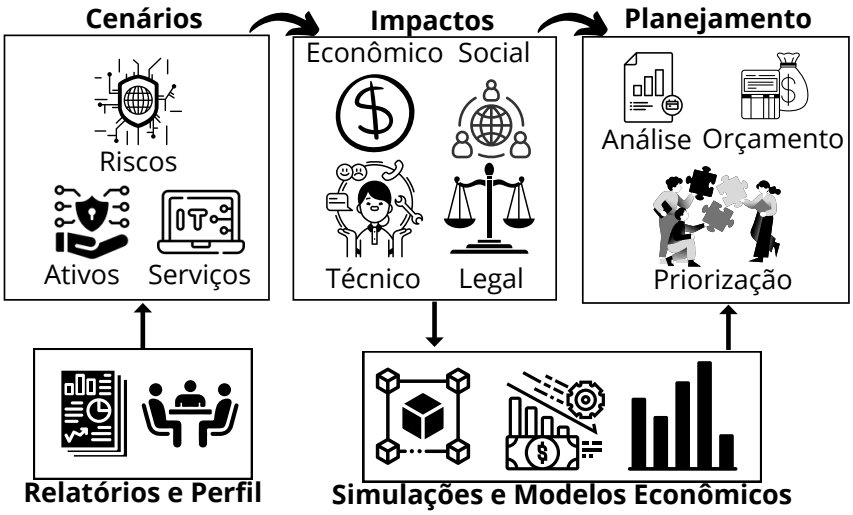

Figura 1. Arquitetura da plataforma IMPACTO.

Durante o uso da plataforma, alunos e instrutores podem modificar os detalhes do cenário para analisar como essas alterações afetam a vulnerabilidade da empresa hipotética e a eficácia dos investimentos em cibersegurança. Uma demonstração da plataforma está disponível publicamente em `https://www.youtube.com/watch?v=x0RAgu_bjSU`.

3.1. Base de Dados de Relatórios da Indústria

A base de dados da plataforma IMPACTO utiliza informações provenientes de relatórios de cibersegurança de empresas renomadas, como os citados em [IBM 2024] e [Verizon 2025]. Essas organizações reúnem dados variados sobre o funcionamento de parceiros, incluindo detalhes técnicos de incidentes, valores de perdas financeiras e

ameaças emergentes. Os dados são organizados conforme o setor de atuação, localização e tipo de ataque sofrido, sendo então armazenados na base de dados da IMPACTO. Exemplos de relatórios utilizados estão listados no Apêndice A.

O banco de dados foi desenvolvido utilizando o framework Django, aproveitando seu sistema de ORM (Object-Relational Mapping) para modelar entidades e relações. Suas principais estruturas incluem: *Scope*, que representa categorias de ameaças cibernéticas; *Region*, que identifica a localização geográfica; e *Sector*, que indica o setor de mercado de origem dos dados. As classes *Report* e *CyberSecurityData* armazenam, respectivamente, metadados sobre as fontes e as métricas probabilísticas usadas na análise de riscos. O diagrama de classes do banco de dados é mostrado na Figura 2.

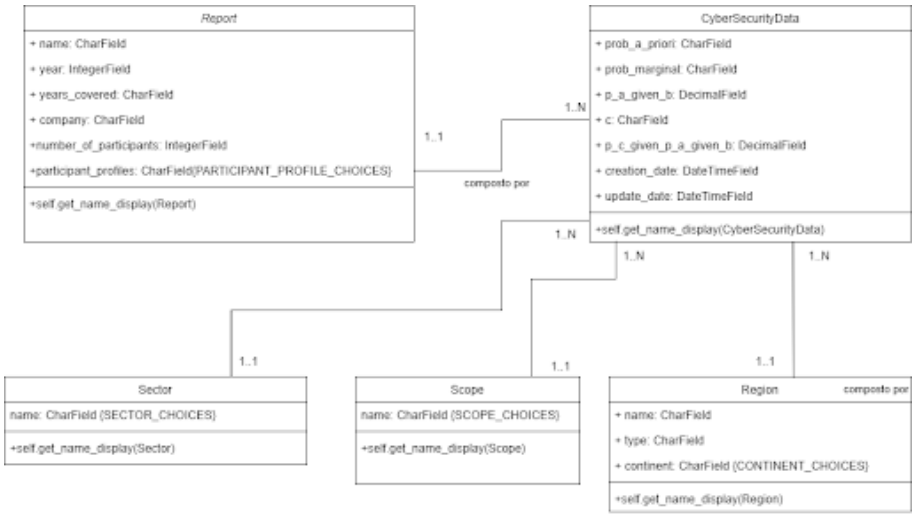

Figura 2. Diagrama de Classes do Banco de Dados de Relatórios.

3.2. Módulo de Análise de Riscos

O Módulo de Análise de Riscos da plataforma IMPACTO possui duas abas principais: *Visão Geral* e *Relatório*. A Figura 5 no Apêndice A mostra uma captura de tela da aba *Visão Geral*, onde os dados dos relatórios alimentam a estimativa da probabilidade de a empresa estudada sofrer ataques como *malware*, *phishing* e DDoS. Essas probabilidades são determinadas levando em conta o setor e a localização da empresa. Além disso, a aba apresenta o perfil da empresa e uma visão geral dos riscos relacionados ao setor e à região. Os alunos podem explorar essas informações para realizar análises sobre o cenário de estudo, sempre com o suporte do instrutor.

Na aba *Relatório*, as probabilidades de ataque previamente calculadas são combinadas aos dados técnicos da empresa para gerar uma análise quantitativa de risco. A Figura 6 no Apêndice A mostra uma captura de tela da página. A plataforma calcula a Pontuação de Risco (PR) [Nunes et al. 2024] a partir de três variáveis principais: setor, região e resiliência. As probabilidades condicionais de ataque para cada tipo de ameaça (*malware*, *phishing* e DDoS) são extraídas do banco de dados com base no setor, país e continente da empresa ($P_{ataque|setor}$, $P_{ataque|pais}$, $P_{ataque|continente}$). Calculam-se a média (M) e o desvio padrão (DP) dessas distribuições, atribuindo à empresa um peso entre 0,3 e 2,0 conforme sua posição relativa, refletindo o risco setorial e regional. Esses processos são descritos na Tabela 3. Um risco mais baixo resulta em uma pontuação PR menor.

A preparação da empresa é avaliada pelas suas práticas de cibersegurança e histórico de incidentes, com pesos atribuídos segundo a eficácia das medidas (impactantes, relevantes ou indiferentes), conforme a Tabela 8 no Apêndice A. O valor final de preparação, entre 0,5 e 4,5, atua como fator de penalização inversa no cálculo da PR.

Após reunir todas as informações, a pontuação de risco de cada tipo de ciberataque é calculada de acordo com as fórmulas da Tabela 3, tendo como referência o valor-base de 6. A média simples dos três resultados fornece a pontuação geral de risco da empresa. A aba *Relatório* também mostra como cada controle de segurança influencia os pilares de confidencialidade, integridade e disponibilidade. Os alunos podem ajustar os controles implementados no cenário da empresa e observar, em tempo real, como essas alterações afetam as pontuações de risco.

Tabela 3. 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	$\min(ValorBase \times Risco_{regiao} \times Risco_{setor} \times Resiliencia,\ 10)$
Pontuação de Risco Geral	$\frac{\sum PR_{ciberataques}}{\sum Ciberataques}$

3.3. Módulo de Planejamento Econômico

A seção de gestão econômica aproveita a pontuação de risco obtida no módulo anterior, aliada aos dados financeiros da empresa. São considerados o valor dos ativos em risco e os investimentos existentes em cibersegurança. Com essas informações, a plataforma orienta didaticamente o usuário sobre qual seria o investimento ideal em medidas de proteção para o cenário analisado.

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 decorrente de um ciberataque, a companhia direcione sua estratégia de investimentos em sistemas de segurança que reduzam 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 módulo de análise de risco, o potencial de perda decorrente de um ciberataque e o valor investido. Por meio dessa modelagem, é possível encontrar o valor de investimento com

melhor rendimento, ou seja, aquele que apresenta o maior ENBIS (*Expected Net Benefit of Information Security*, benefício líquido esperado) considerando o custo do investimento.

A página de Gestão Econômica é composta por duas seções. A primeira apresenta uma tabela que analisa a eficiência dos investimentos e sugere ajustes para atingir o ENBIS máximo em cada tipo de ataque. A segunda seção exibe um gráfico do EBIS em relação ao valor investido, destacando os investimentos atuais, os ótimos e se o valor aplicado está dentro do intervalo adequado. A Figura 7 no Apêndice A mostra uma captura de tela da página de Gestão Econômica.

Alunos e instrutores podem ajustar os parâmetros de simulação, comparando diferentes estratégias de investimento em cibersegurança. Na janela ”Impactos”(Figura 3), os impactos dos ataques podem ser classificados como altos, médios ou baixos para cada situação. Por exemplo, um ataque de ”Malware”pode afetar severamente um servidor, enquanto ”Phishing”pode ter impacto menor no mesmo ativo. Os danos esperados são recalculados conforme cada nível de impacto. No modo ”Simulação Avançada”, é possível modificar manualmente valores de dano, probabilidade e investimento, além de recalcular as equações do modelo de Gordon-Loeb (Figura 4). Isso permite que instrutores criem variações de exercícios e que alunos avaliem as consequências de suas decisões em diferentes cenários.

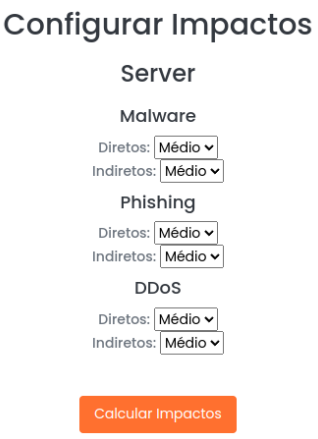

Figura 3. Janela para configuração do impacto de um ataque com sucesso no valor do ativo.

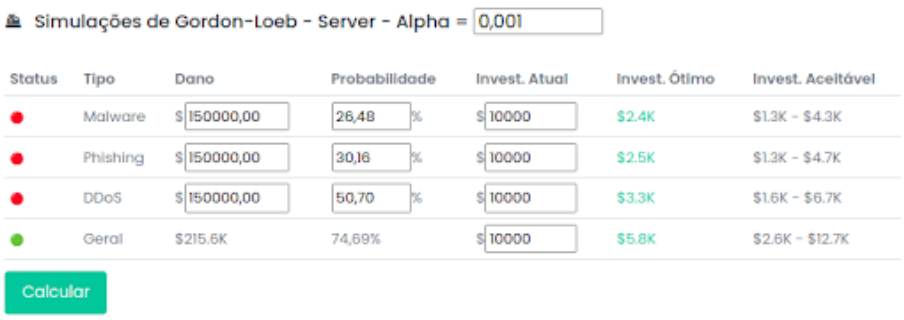

Figura 4. Ferramenta para simulação de cenários avançados.

4. Avaliação

A plataforma IMPACTO foi testada por alunos do Programa Hackers do Bem, além de estudantes de graduação e pós-graduação em áreas relacionadas à cibersegurança. Ao todo, participaram 28 pessoas com idades entre 20 e 40 anos. O objetivo da avaliação foi verificar se as funcionalidades principais da plataforma ajudam os usuários nas tarefas de planejamento e análise econômica em cibersegurança. Também foi realizada uma análise de usabilidade utilizando o método System Usability Score (SUS) com os mesmos participantes.

4.1. Casos de Uso e Demonstração

A avaliação seguiu uma sequência estruturada de atividades, embora não obrigatória para o uso da plataforma. O processo envolveu: (i) identificar o ataque cibernético mais relevante na página *Visão Geral*; (ii) consultar a página *Relatório* para determinar o nível de resiliência da empresa; (iii) simular cenários criando cópias e ajustando medidas de cibersegurança; (iv) realizar análise econômica e conferir no módulo de Gestão Econômica se o investimento atual está alinhado ao valor ótimo segundo o modelo Gordon-Loeb; e (v) explorar a seção *Fonte de Dados* para identificar setores mais vulneráveis a ataques específicos.

4.2. Questionários

Depois de realizadas as atividades usando a plataforma, os participantes foram convidados a responder um formulário de usabilidade sobre a experiência com a ferramenta. Foi utilizado um questionário no modelo SUS (do inglês *System Usability Scale*, ou escala de usabilidade do sistema) [Brooke et al. 1996]. Nesse questionário, os participantes recebem um conjunto de 10 afirmações sobre a experiência de uso do sistema e atribuem notas de 1 (discorda totalmente) a 5 (concorda totalmente). As questões que fazem parte do questionário estão na Tabela 4.

Tabela 4. Questionário de usabilidade no modelo SUS que foi utilizado durante a avaliação.

#	Descrição
S1	Eu gostaria de usar esse sistema com frequência.
S2	Eu achei o sistema desnecessariamente complexo.
S3	Eu achei o sistema fácil de usar.
S4	Eu penso que eu precisaria de suporte de um técnico para conseguir usar esse sistema.
S5	Eu achei que as várias funções desse sistemas estão bem integradas.
S6	Eu achei que existiam muitas inconsistências nesse sistema.
S7	Eu imagino que a maioria das pessoas conseguiria aprender a usar esse sistema muito rapidamente.
S8	Eu achei o sistema muito incômodo de se usar.
S9	Eu me senti muito confiante usando o sistema.
S10	Eu precisei aprender muitas coisas antes de conseguir começar a usar esse sistema.

Depois da avaliação de usabilidade, foi feita uma avaliação de adequação à grade curricular do programa Hackers do Bem. Para tanto, foi aplicado um questionário de adequação elaborado pelos autores, disponível na Tabela 5, seguindo o mesmo formato usado pelo questionário SUS de atribuição de notas de 1 a 5 para afirmações sobre a adequação do conteúdo abordado pela plataforma.

Tabela 5. Questionário de adequação à grade curricular do programa Hackers do Bem, de autoria própria.

#	Descrição
I1	O conteúdo que estudei até o momento no programa Hackers do Bem foi suficiente para eu conseguir usar o sistema.
I2	Os tópicos abordados pelo sistema contribuem positivamente para a minha formação.
I3	Eu achei o nível dos conhecimentos abordados muito básico.

4.3. Resultados

A avaliação da IMPACTO contou com 28 participantes: 20 do programa Hackers do Bem (71,4%) e 8 de outras instituições, sobretudo do ensino superior. O processo foi dividido em quatro etapas: preparação com consentimento e coleta de dados demográficos, avaliação de funcionalidades via exercícios práticos, aplicação do questionário SUS para usabilidade e, devido ao foco educacional, avaliação de adequação curricular para os participantes do Hackers do Bem.

Os exercícios de funcionalidade abrangeram desde a navegação básica até análises econômicas mais avançadas. A Tabela 6 mostra exemplos de atividades realizadas e as respectivas taxas de acerto, evidenciando a eficácia da IMPACTO como ferramenta educacional. A média geral de acertos foi de 93,45%. Enquanto as funções básicas de visualização e análise tiveram excelente desempenho, recursos mais complexos, como a duplicação de cenários e o detalhamento de valores monetários, apontaram oportunidades de aprimoramento.

Tabela 6. 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%

O questionário SUS gerou uma pontuação média de 85,28, considerada excelente e equivalente à nota A+ em usabilidade. Esse resultado demonstra que a plataforma possui alta usabilidade, interface intuitiva e alto grau de satisfação dos usuários, sendo adequada para contextos educacionais. Na avaliação curricular, os participantes do Hackers do Bem julgaram o conteúdo relevante e alinhado à formação em cibersegurança e economia. O *feedback* qualitativo foi majoritariamente positivo, destacando a interface intuitiva, a utilidade dos recursos e sugerindo melhorias construtivas.

A avaliação com usuários do público-alvo da IMPACTO possibilitou validar as funcionalidades já implementadas e identificar melhorias para versões futuras. O *feedback* dos participantes apontou, por exemplo, a necessidade de tornar as informações do módulo de gestão econômica mais organizadas para facilitar a experiência do usuário.

Outras sugestões incluem a adição de recursos para comparar cenários antes e depois das alterações feitas pelos alunos.

5. Considerações Finais

A plataforma IMPACTO foi criada para suprir a demanda por soluções que facilitem a compreensão dos aspectos econômicos dos ciberataques, promovam a análise de riscos e apoiem o planejamento de investimentos em cibersegurança. Seu principal diferencial está na capacitação de profissionais por meio de cenários de treinamento, tornando claros e acessíveis os modelos e conceitos envolvidos. A estrutura modular possibilita adaptação a diferentes níveis educacionais, desde aulas introdutórias até análises aprofundadas em planejamento econômico. A avaliação de usabilidade apontou alto índice de sucesso nas tarefas, evidenciando o potencial da ferramenta para desenvolver competências analíticas em cibersegurança e economia.

Como próximos passos, ideias possíveis são a criação de um módulo para recomendar proteções com base em orçamentos definidos, além da integração com métricas técnicas de priorização de riscos, como o *Exploit Prediction Scoring System* (EPSS). Outro passo recomentados antes do *deploy* em uma instituição seria o desenvolvimento de cenários específicos para a demanda em questão, principalmente se tratando da capacitação de profissionais de cibersegurança para setores críticos, como Saúde [Franco et al. 2025] e Financeiro [Gulyas and Kiss 2023], que demandam maior eficiência econômica no planejamento de suas estratégias.

Agradecimentos

O presente trabalho foi realizado com o apoio do Programa Hackers do Bem no Domínio Cibernético, executado pela RNP e SENAI, coordenado pela Softex e financiado pelo MCTI com recursos oriundos da Lei das TICs – Lei nº 8.248, de 23 de outubro de 1991.

Referências

Aiyer, B., Caso, J., Russell, P., and Sorel, M. (2022). New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers. Acesso em Dezembro de 2024.

Brooke, J. et al. (1996). Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7.

European Commission (2020). Skills for SMEs: Cybersecurity, Internet of things and big data for small and medium-sized enterprises. https://data.europa.eu/doi/10.2826/708138. Acesso em Dezembro de 2024.

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 7. 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 8. 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

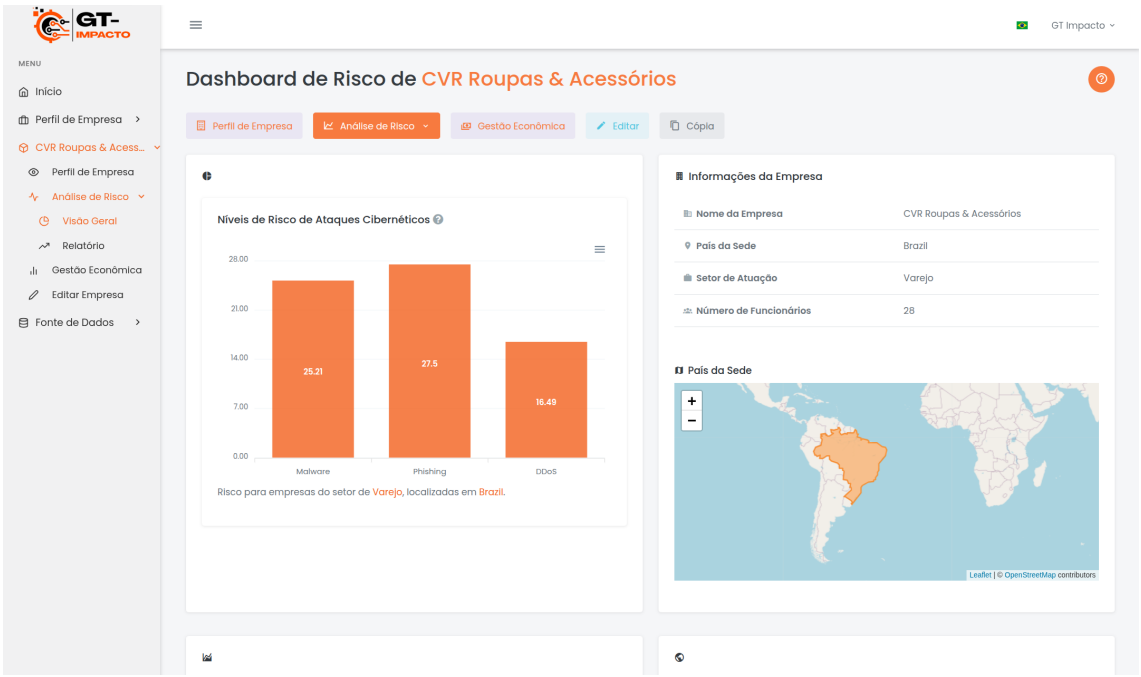

Figura 5. Captura de tela do módulo de Análise de Riscos, na aba *Visão Geral*.

Figura 6. Captura de tela do módulo de Análise de Riscos, na aba *Relatório*.

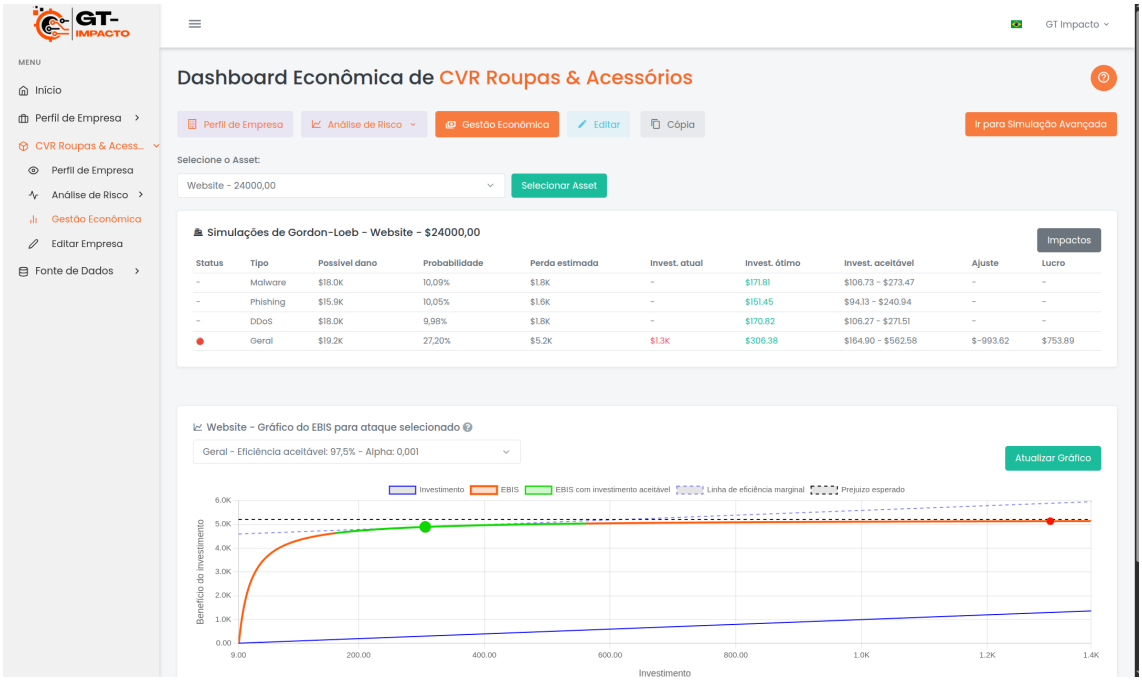

Figura 7. Captura de tela da página de Planejamento Econômico.