

Otimização de Investimentos em Cibersegurança Sob Restrições Orçamentárias

Alexandre Ramos do Nascimento¹, José Antonio Moreira Xexéo¹,
Raquel Coelho Gomes Pinto¹, Anderson Fernandes Pereira dos Santos^{1,2}

¹Instituto Militar de Engenharia (IME) – Rio de Janeiro – RJ

²Venturus Centro de Inovação – Campinas – SP

{alexandre.ramos, xexeo, raquel, anderson}@ime.eb.br

Abstract. *Cybersecurity controls compete for limited organizational budgets. This paper formulates their selection as a 0/1 Knapsack Problem, combining implementation cost, effectiveness, operational impact, asset criticality, and MITRE ATT&CK coverage derived from CIS Controls v8. The binary model is converted into QUBO and then into an Ising cost Hamiltonian with a budget penalty and slack variables. The contribution provides a common formulation for classical optimization and future QAOA experiments, without assuming quantum advantage.*

Keywords *Cybersecurity; Optimization; Security Controls; QUBO; QAOA.*

Resumo. *Controles de cibersegurança competem por orçamentos organizacionais limitados. Este artigo formula sua seleção como um Problema da Mochila 0/1, combinando custo de implementação, eficácia, impacto operacional, criticidade dos ativos e cobertura MITRE ATT&CK derivada dos CIS Controls v8. O modelo binário é convertido em QUBO e, depois, em um Hamiltoniano de custo Ising com penalidade orçamentária e variáveis de folga. A contribuição fornece uma formulação comum para otimização clássica e futuras avaliações com QAOA, sem pressupor vantagem quântica.*

Palavras-Chave *Cibersegurança; Otimização Combinatória; Controles de Segurança; QUBO; QAOA.*

1. Introdução

A priorização de investimentos em cibersegurança exige escolher controles concorrentes sob orçamento limitado, equilibrando custo, risco e efetividade [Gordon e Loeb 2002]. Este trabalho modela essa decisão como um Problema da Mochila 0/1: cada controle possui custo e valor de segurança, e busca-se selecionar o subconjunto de maior valor sem exceder o orçamento.

A contribuição consiste em relacionar controles do CIS Controls v8 a táticas do MITRE ATT&CK, definir uma métrica normalizada de valor de segurança e converter o problema para QUBO e para um Hamiltoniano de custo compatível com QAOA [Farhi et al. 2014]. O artigo apresenta os trabalhos relacionados, a formulação matemática, a derivação do Hamiltoniano e suas limitações.

2. Trabalhos Relacionados

[Gordon e Loeb 2002] analisam o nível econômico de investimento. [Fielder et al. 2016] e [Panda et al. 2020] combinam teoria dos jogos e mochila. [Sawik 2022] emprega programação inteira, enquanto [Sawik e Sawik 2022] trata portfólios binários. [Tsiodra et al. 2023] compara mochila e cobertura de conjuntos.

Na vertente quântica, [Giraldo-Osorio et al. 2024] aplicam VQE e QAOA à alocação de recursos, e [Guney et al. 2025] modelam o Problema das Múltiplas Mochilas por meio de uma formulação QUBO. [Christiansen et al. 2025] usam estados factíveis e misturadores específicos, enquanto [Bucher et al. 2025] evitam penalidades QUBO convencionais. Essas propostas não integram CIS Controls v8 e MITRE ATT&CK na seleção de controles.

A lacuna identificada é a ausência de uma formulação que integre controles reais, cobertura de ameaças, criticidade, eficácia, impacto operacional e orçamento em um Hamiltoniano de custo. A Tabela 1 resume o posicionamento da proposta.

Tabela 1. Comparação entre trabalhos relacionados e critérios abordados.

Trabalho	Seleção de Controles	Otimização Clássica	Otimização Quântica (QAOA+QUBO)	Otimização Quântica (Outros)
Gordon e Loeb (2002)	Não	Sim	Não	Não
Fielder et al. (2016)	Sim	Sim	Não	Não
Panda et al. (2020)	Sim	Sim	Não	Não
Sawik (2022)	Sim	Sim	Não	Não
Sawik e Sawik (2022)	Sim	Sim	Não	Não
Tsiodra et al. (2023)	Sim	Sim	Não	Não
Giraldo-Osorio et al. (2024)	Não	Não	Sim	Não
Bucher et al. (2025)	Não	Não	Não	Sim
Christiansen et al. (2025)	Não	Não	Não	Sim
Guney et al. (2025)	Não	Não	Sim	Não
Este Trabalho	Sim	Não	Sim	Não

3. Proposta do Trabalho

3.1. Escopo e Controles Considerados

O modelo proposto apoia a escolha de um subconjunto de controles de cibersegurança quando o orçamento disponível não permite implementar todos os controles. Cada controle é tratado como uma decisão indivisível, associada a um custo de implementação e a um valor de segurança. Esse valor representa não apenas sua eficácia técnica, mas também sua aderência às ameaças relevantes, sua importância para os ativos protegidos e o impacto operacional decorrente de sua adoção.

Adota-se o CIS Controls v8, com foco no IG1, que reúne salvaguardas prioritárias [Center for Internet Security 2021]. Os controles são relacionados às táticas potencialmente mitigadas do MITRE ATT&CK [MITRE Corporation 2024]. A Tabela 2 apresenta esse mapeamento, que adapta a prioridade ao perfil de ameaças. A instância é ilustrativa e admite outros controles, ativos e táticas.

Tabela 2. Controles CIS e táticas MITRE ATT&CK associadas.

Controle CIS v8	Táticas MITRE ATT&CK
CIS-1: Inventário de hardware	Reconnaissance; Initial Access
CIS-2: Inventário de software	Execution; Persistence
CIS-4: Configuração segura	Persistence; Defense Evasion
CIS-5: Gestão de contas	Privilege Escalation; Lateral Movement
CIS-7: Gestão de vulnerabilidades	Initial Access; Execution
CIS-9: Proteção de e-mail e navegador	Initial Access; Execution
CIS-10: Defesa contra malware	Execution; Collection; Exfiltration

3.2. Formulação Matemática

Sejam $\mathcal{C}$, $\mathcal{A}$ e $\mathcal{M}$ os conjuntos de controles, ativos e táticas MITRE ATT&CK, respectivamente. Para cada controle $i \in \mathcal{C}$, $x_i \in \{0, 1\}$ indica sua seleção, $c_i \in \mathbb{R}^+$ representa o custo direto de implementação, $f_i \in [0, 1]$ seu impacto operacional normalizado, $e_i \in [0, 1]$ sua eficácia técnica e $p_i \in [0, 1]$ sua prioridade segundo o CIS Controls.

Para representar o componente humano, define-se $h_i \in [0, 1]$ como o nível esperado de adesão de usuários e operadores ao controle. A eficácia efetiva é, então,

$$\tilde{e}_i = e_i h_i. \quad (1)$$

Assim, um controle tecnicamente eficaz pode receber menor valor quando sua aplicação depender de comportamentos, treinamento ou procedimentos com baixa adesão. O impacto operacional f_i complementa essa representação ao considerar fatores como esforço de treinamento, sobrecarga de trabalho, redução de produtividade e possibilidade de contorno do controle.

A criticidade direta de cada ativo $j \in \mathcal{A}$ é construída a partir de diferentes dimensões de impacto. Seja $\mathcal{H}$ o conjunto formado, por exemplo, pelos impactos financeiro, operacional, regulatório, reputacional e humano. Define-se

$$v_j^{(0)} = \sum_{h \in \mathcal{H}} \omega_h v_{jh}, \quad \sum_{h \in \mathcal{H}} \omega_h = 1, \quad \omega_h \geq 0, \quad (2)$$

em que $v_{jh} \in [0, 1]$ representa o impacto do comprometimento do ativo j na dimensão h . Essa decomposição permite incorporar fatores que não possuem mensuração monetária direta, como reputação, marca, confiança dos usuários e consequências sobre pessoas.

Para representar efeitos indiretos, seja $d_{j\ell} \in [0, 1]$ o impacto do comprometimento do ativo j sobre ℓ . A criticidade propagada é

$$\tilde{v}_j = \frac{v_j^{(0)} + \eta \sum_{\ell \neq j} d_{j\ell} v_\ell^{(0)}}{1 + \eta \sum_{\ell \neq j} d_{j\ell}}, \quad 0 \leq \eta \leq 1, \quad (3)$$

em que $\eta = 0$ considera somente o impacto direto, enquanto valores maiores incorporam efeitos em cascata. Sejam $r_j \in [0, 1]$ a exposição do ativo, $z_{ij} \in \{0, 1\}$ a relação entre controle e ativo, $m_{ik} \in \{0, 1\}$ a relação entre controle e tática, e $q_k \in [0, 1]$ a relevância

da tática. Definem-se

$$a_i = \frac{\sum_{k \in \mathcal{M}} q_k m_{ik}}{\sum_{k \in \mathcal{M}} q_k}, \quad u_i = \frac{\sum_{j \in \mathcal{A}} z_{ij} \tilde{v}_j r_j}{\sum_{j \in \mathcal{A}} z_{ij}}, \quad w_i = \lambda p_i + (1 - \lambda) u_i, \quad (4)$$

com $0 \leq \lambda \leq 1$ e $u_i = 0$ quando $\sum_j z_{ij} = 0$. O parâmetro λ equilibra a prioridade CIS e a relevância dos ativos, enquanto q_k pondera as táticas segundo o contexto organizacional.

O valor de segurança do controle é

$$R_i = \alpha \tilde{e}_i + \beta a_i + \gamma w_i + \delta(1 - f_i), \quad \alpha + \beta + \gamma + \delta = 1, \quad (5)$$

com pesos não negativos e $R_i \in [0, 1]$. A métrica explicita os compromissos entre eficácia, cobertura, criticidade e impacto operacional. Para $\alpha = 1$, a seleção considera apenas a eficácia; com os demais pesos positivos, controles de menor eficácia podem ser priorizados por sua maior cobertura, criticidade ou menor impacto.

Por exemplo, para controles de mesmo custo e pesos iguais, considere

$$\mathbf{r}_A = (0,9, 0,3, 0,4, 0,1), \quad \mathbf{r}_B = (0,7, 0,8, 0,8, 0,2), \quad (6)$$

em que $\mathbf{r}_i = (\tilde{e}_i, a_i, w_i, f_i)$. Obtêm-se $R_A = 0,625$ e $R_B = 0,775$. Uma seleção baseada apenas em eficácia escolheria A , enquanto a métrica proposta priorizaria B . O exemplo ilustra o efeito da métrica, sem evidenciar superioridade empírica.

O modelo básico é uma instância da Mochila 0/1 [Martello e Toth 1990]. A formulação também segue Kellerer et al. [Kellerer et al. 2004]:

$$\max_{\mathbf{x}} V(\mathbf{x}) = \sum_{i \in \mathcal{C}} R_i x_i \quad \text{s.a.} \quad \sum_{i \in \mathcal{C}} c_i x_i \leq B, \quad x_i \in \{0, 1\}. \quad (7)$$

A função objetivo maximiza o valor agregado dos controles selecionados, enquanto a restrição assegura que o custo total permaneça dentro do orçamento B .

A viabilidade orçamentária não garante um portfólio aceitável. Define-se a cobertura da tática k por $g_k(\mathbf{x}) = \min\{1, \sum_i m_{ik} x_i\}$ e a cobertura ponderada por

$$A(\mathbf{x}) = \frac{\sum_{k \in \mathcal{M}} q_k g_k(\mathbf{x})}{\sum_{k \in \mathcal{M}} q_k}, \quad V(\mathbf{x}) \geq V_{\min}, \quad A(\mathbf{x}) \geq A_{\min}. \quad (8)$$

Os limiares $V_{\min}$ e $A_{\min}$ representam os níveis mínimos de valor e cobertura definidos pela organização.

Quando nenhuma solução satisfaz simultaneamente (7) e (8), o resultado deve ser interpretado como evidência de que o orçamento disponível é insuficiente para atingir o nível de segurança estabelecido. Portanto, o modelo não pressupõe que qualquer solução dentro do orçamento seja necessariamente segura.

As condições de aceitabilidade podem ser verificadas após a otimização ou incorporadas como restrições adicionais, mediante linearização das variáveis g_k . Nesse segundo caso, o problema deixa de ser uma mochila 0/1 simples e passa a constituir uma formulação binária com múltiplas restrições.

3.3. Hamiltoniano de Custo

A conversão para QUBO considera o modelo da Equação (7). Introduce-se a folga $s = \sum_{m=0}^{M-1} 2^m y_m$, com $y_m \in \{0, 1\}$ e $M = \lceil \log_2(B + 1) \rceil$, para transformar a restrição orçamentária em igualdade. Admitindo c_i e B discretizados em uma unidade inteira comum, obtém-se

$$Q(\mathbf{x}, \mathbf{y}) = - \sum_{i \in \mathcal{C}} R_i x_i + \rho \left(\sum_{i \in \mathcal{C}} c_i x_i + \sum_{m=0}^{M-1} 2^m y_m - B \right)^2, \quad (9)$$

em que $\rho > 0$ penaliza violações do orçamento. Para uma violação mínima unitária, pode-se adotar $\rho > \sum_{i \in \mathcal{C}} R_i$. Valores baixos podem favorecer soluções inviáveis, enquanto valores elevados podem dificultar a otimização numérica. As condições da Equação (8) são verificadas separadamente, pois sua inclusão exigiria penalidades e variáveis auxiliares adicionais.

Aplicando $x_i = (\mathbb{I} - Z_i)/2$ e $y_m = (\mathbb{I} - Z_m^{(y)})/2$ [Farhi et al. 2014], obtém-se

$$H_C = - \sum_{i \in \mathcal{C}} R_i \frac{\mathbb{I} - Z_i}{2} + \rho \left(\sum_{i \in \mathcal{C}} c_i \frac{\mathbb{I} - Z_i}{2} + \sum_{m=0}^{M-1} 2^m \frac{\mathbb{I} - Z_m^{(y)}}{2} - B \right)^2. \quad (10)$$

Definindo $D = \frac{1}{2}(\sum_i c_i + \sum_m 2^m) - B$ e descartando constantes globais, o Hamiltoniano assume a forma Ising [Lucas 2014, Glover et al. 2019]:

$$H_C = \sum_i h_i^{(x)} Z_i + \sum_m h_m^{(y)} Z_m^{(y)} + \sum_{i < j} J_{ij}^{(xx)} Z_i Z_j + \sum_{i, m} J_{im}^{(xy)} Z_i Z_m^{(y)} + \sum_{m < r} J_{mr}^{(yy)} Z_m^{(y)} Z_r^{(y)}. \quad (11)$$

Os campos locais e acoplamentos são

$$\begin{aligned} h_i^{(x)} &= \frac{R_i}{2} - \rho D c_i, & h_m^{(y)} &= -\rho D 2^m, & J_{ij}^{(xx)} &= \frac{\rho}{2} c_i c_j, \\ J_{im}^{(xy)} &= \frac{\rho}{2} c_i 2^m, & J_{mr}^{(yy)} &= \frac{\rho}{2} 2^{m+r}. \end{aligned} \quad (12)$$

O operador contém campos locais em Pauli- Z e acoplamentos ZZ , compatíveis com o QAOA. O modelo requer $n + M$ qubits: n para os controles e M para a folga. Essa compatibilidade não implica maior eficiência que a resolução clássica, pois a codificação, as penalidades e a conectividade podem elevar a profundidade e o número de portas.

3.4. Análise e Limitações

A proposta conecta modelos clássicos de investimento em cibersegurança a formulações quânticas para o Problema da Mochila. Sua contribuição consiste em definir uma métrica multicritério baseada em controles CIS, ativos organizacionais, fatores humanos e táticas MITRE ATT&CK, além de construir um Hamiltoniano associado a esse problema. Entretanto, R_i não garante melhoria sobre funções tradicionais; seus efeitos devem ser avaliados por comparação experimental.

A validação deverá comparar a métrica proposta com critérios baseados apenas em eficácia ou na razão entre valor e custo, empregando programação inteira, métodos exatos, heurísticas e metaheurísticas como referências clássicas. A análise deve considerar valor objetivo, cobertura de ameaças, proteção de ativos críticos, factibilidade, lacuna

de otimalidade, tempo de execução e escalabilidade. Para o QAOA, também devem ser medidos número de qubits, profundidade do circuito, quantidade de portas e avaliações da função objetivo.

Métodos clássicos consolidados podem ser mais simples e eficientes, especialmente em instâncias pequenas e médias. O uso do QAOA somente será justificável se apresentar ganhos relevantes em qualidade, tempo ou escalabilidade. Além disso, sua adoção envolve ruído, conectividade limitada, custo de execução, acesso restrito ao hardware e necessidade de conhecimento especializado.

O modelo também depende de parâmetros organizacionais e avaliações subjetivas. Valores relacionados à eficácia, criticidade, exposição, relevância das ameaças, impacto operacional, adesão humana e dependência entre ativos estão sujeitos a incerteza. A representação atual não captura completamente mudanças comportamentais, falhas em cascata, relações não lineares, redundâncias ou sinergias entre controles, devendo essas questões ser tratadas por análises de sensibilidade e extensões da função objetivo.

Por fim, uma solução ótima dentro do orçamento não é necessariamente segura. Os limiares $V_{\min}$ e $A_{\min}$ devem representar níveis mínimos aceitáveis de valor e cobertura; caso não possam ser atendidos, o resultado deve indicar insuficiência orçamentária. Este trabalho é exploratório e apresenta apenas a formulação e o Hamiltoniano, sem implementação, comparação empírica ou evidência de vantagem quântica.

4. Considerações Finais

Este artigo apresentou uma formulação para selecionar controles de cibersegurança sob restrição orçamentária, integrando CIS Controls v8, ativos e táticas MITRE ATT&CK em uma métrica normalizada. O problema foi modelado como Mochila 0/1, convertido em QUBO e mapeado para um Hamiltoniano Ising, permitindo resolução clássica e futura avaliação com QAOA.

Na taxonomia de [Al Salek et al. 2026] (ainda não publicada), a proposta caracteriza-se como um modelo não canônico, estático, de ator único e escopo de portfólio, orientado pelo compromisso entre custo e benefício. Como a taxonomia não contempla modelos quânticos, o QUBO e o QAOA são tratados aqui como uma camada computacional para representar e solucionar o modelo de seleção. Este trabalho exploratório limita-se à modelagem, sem resultados experimentais ou evidências de vantagem quântica. As próximas etapas incluem parametrização com dados organizacionais, validação do mapeamento, comparação com métodos clássicos e avaliação do QAOA quanto à qualidade, factibilidade, tempo, número de qubits e escalabilidade.

Declaração de Uso de Inteligência Artificial Generativa

Em conformidade com o Código de Conduta para Autores da SBC (2024), declara-se que ferramentas de IA generativa, incluindo ChatGPT (OpenAI), foram utilizadas como apoio à revisão linguística e à formatação. As decisões metodológicas, a formulação matemática e a responsabilidade pelo conteúdo são dos autores.

Referências

Al Salek, A., Padyab, A., Lundgren, M., e Ahlfeldt, R.-M. (2026). A taxonomy of cybersecurity economic models. *Computers & Security*. In press.

- Bucher, D., Stein, J., Feld, S., e Linnhoff-Popien, C. (2025). Penalty-free approach to accelerating constrained quantum optimization. *Physical Review A*, 112(6):062605.
- Center for Internet Security (2021). CIS Controls Version 8. <https://www.cisecurity.org/controls/v8>.
- Christiansen, P., Binkowski, L., Ramacciotti, D., e Wilkening, S. (2025). Quantum tree generator improves QAOA state-of-the-art for the knapsack problem. In Culhane, C., Byrd, G., Muller, H., Delgado, A., e Eidenbenz, S., editors, *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE.
- Farhi, E., Goldstone, J., e Gutmann, S. (2014). A quantum approximate optimization algorithm. arXiv:1411.4028 [quant-ph].
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., e Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23.
- Giraldo-Osorio, A., Navarrete, A., Griol, D., e Calvo-Manzano, J. A. (2024). Quantum computing for resource allocation in cloud-edge environments: A VQE and QAOA approach. *IEEE Access*, 12:30030–30044.
- Glover, F., Kochenberger, G., e Du, Y. (2019). Quantum bridge analytics I: A tutorial on formulating and using QUBO models. *4OR: A Quarterly Journal of Operations Research*, 17(4):335–371.
- Gordon, L. A. e Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457.
- Guney, E., Ehrenthal, J., e Hanne, T. (2025). Quantum approaches to the 0/1 multi-knapsack problem: QUBO formulation, penalty parameter characterization and analysis. In *Proceedings of the 17th International Conference on Agents and Artificial Intelligence*, volume 1 of *QAIO*, pages 815–823. INSTICC, SciTePress.
- Kellerer, H., Pferschy, U., e Pisinger, D. (2004). *Knapsack Problems*. Springer, Berlin.
- Lucas, A. (2014). Ising formulations of many NP problems. *Frontiers in Physics*, 2:5.
- Martello, S. e Toth, P. (1990). *Knapsack Problems: Algorithms and Computer Implementations*. Wiley, Chichester.
- MITRE Corporation (2024). MITRE ATT&CK: Adversarial Tactics, Techniques and Common Knowledge. <https://attack.mitre.org>.
- Panda, S., Panaousis, E., Loukas, G., e Laoudias, C. (2020). Optimizing investments in cyber hygiene for protecting healthcare users. Preprint.
- Sawik, T. (2022). A linear model for optimal cybersecurity investment in industry 4.0 supply chains. *International Journal of Production Research*, 60(4):1368–1385.
- Sawik, T. e Sawik, B. (2022). A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. *International Journal of Production Research*, 60(21):6556–6572.
- Tsiodra, M., Panda, S., Chronopoulos, M., e Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. *IEEE Access*, 11:44467–44481.