**Instituto de Informática (INF)**
Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS
URL: https://www.inf.ufrgs.br

**Orientador:** Prof. Dr. Lisandro Zambenedetti Granville
**Coorientador:** Dr. Muriel Figueredo Franco
Grupo de Redes de Computadores
E-mail: [granville, mffranco]@inf.ufrgs.br

# Uma Abordagem Quantitativa para Análise da Eficácia de Medidas de Cibersegurança em Redes de Computadores Corporativas

## 1 Introdução e Motivação

Cibersegurança envolve a análise de diferente dimensões e impactos, como por exemplo técnicos, econômicos, jurídicos e sociais. É cada vez mais necessário que o planejamento adequado de estratégias de cibersegurança levem em conta tais dimensões [1]. Porém, o acesso e manipulação de informações relativas a impactos de ciberataques não é uma tarefa fácil. Empresas tendem a não compartilhar informações de forma pública e também adotam um comportamento pouco colaborativo em relação a ameaças e seus impactos [2]. Portanto, embora necessário, abordagens que permitam quantificar os reais impactos de ciberataques, bem como a real eficiência de controles de segurança, são escaças. De modo a suprir a limitação de informações e suas complexidades, simulações (*e.g.,* What-If, Monte Carlo e Cadeias de Markov) e modelos estocástico têm sido usado por abordagens de cibersegurança [3, 4] como um caminho para integrar e mensurar aspectos socioeconômicos da cibersegurança, incluindo análise de riscos [5] e avaliação de medidas de segurança [6].

O foco deste trabalho de conclusão é propor uma abordagem, baseada em simulações e estatísticas de cibersegurança, para a modelagem de impactos de ameaças cibernéticas e medidas de prevenção. Com isso, espera-se ser possível quantificar a eficácia e viabilidade (técnica e econômica) de diferentes medidas de proteção de forma inovadora e efetiva. O foco será em ameaças e custos em redes corporativas, de modo a contribuir com atividades de planejamento e investimento em cibesegurança por empresas no mundo real.

## 2 Descrição das Atividades

As atividades a serem desenvolvidas durante o TG1 e TG2 são descritas abaixo. Porém, tais atividades podem ser alteradas de acordo com a necessidade durante o desenvolvimento do trabalho.

A1. **Estudo de Conceitos de Cibersegurança (e.g., Ameaças, Proteções e Impactos):** Essa atividade deve ser conduzida de modo ao/a aluno(a) familiarizar-se com o tópico do trabalho e seus principais fundamentos. Tópicos chaves para estudo serão discutidas com o orientador nas reuniões iniciais.

A2. **Revisão Bibliográfica sobre Quantificação de Riscos Cibernéticos e Simulações para Cibersegurança:** Após o entendimento dos conceitos chaves, o/a aluno(a) deverá analisar artigos científicos relacionados a análise quantitativa de riscos (técnicos e econômicos), especialmente artigos que utilizem técnicas simulações como ferramenta para solução de problemas identificados na área.

A3. **Definição da Abordagem:** O/A aluno(a) deverá ser capaz, juntamente com os orientadores, de propor uma abordagem eficaz para resolver problemas previamente identificados na literatura de forma inovadora e eficaz. A abordagem deverá explorar técnicas de simulação para mensurar a eficácia de proteções em relação a aspectos técnicos e socioecônomicos, o qual poderá ser baseado em dados reais ou hipotéticos definidos conforme literatura especializada.

A4. **Design e Implementação de um Protótipo:** Após a definição da abordagem, uma solução deverá ser proposta e implementada como prova de conceito. A solução permitirá mostrar a aplicação do modelo em diferentes cenários definidos pelo(a) aluno(a). A implementação poderá utilizar diferentes tecnologias e técnicas de engenharia de software previamente definidas com os orientadores.

A5. **Avaliação da Abordagem Proposta:** A solução deverá ser analisada de forma quantitativa e/ou qualitativa. As avaliações serão definidas juntamente com os orientadores, de forma a alcançar os melhores resultados possíveis dentro do prazo de execução do trabalho.

A6. **Escrita do Trabalho de Conclusão:** Essa atividade é continua e deverá ser realizada ao longo de todo o trabalho, conforme discussão e cronograma definido com os orientadores. O Trabalho de Conclusão deverá apresentar de forma clara e completa o trabalho proposto e seu desenvolvimento.

As atividades deverão ser realizadas ao longo de 1 (um) ano durante as cadeiras de Trabalho de Graduação (TG) 1 e 2. As atividades de escrita deverão ocorrer em paralelo com o desenvolvimento prático do trabalho. Sugere-se que os seguintes capítulos estejam concluídos ao final de cada uma das cadeiras:

- **TG1**: Introdução e Motivação, Referencial Teórico e Trabalhos Relacionados;

- **TG2**: Abordagem, Implementações, Avaliações e Conclusões.

Porém, tais atividades e entregas poderão ser alteradas se acordadas com os orientadores para um melhor desenvolvimento do trabalho e adequação a metas/resultados do trabalho.

## 3 Requisitos

- Conceitos básicos de cibersegurança
- Interesse por estratégias de cibersegurança
- Interesse por redes de computadores
- Capacidade para leitura de artigos em Inglês (Desejável mas não obrigatório);

## References


[1] M. F. Franco, "CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment," February 2023, PhD Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, Available at https://figueredofranco.com/static/files/PhD-M-Franco.pdf.

[2] Y. Wu, M. Xu, D. Cheng, and T. Dai, "Information Security Strategies for Information-Sharing Firms Considering a Strategic Hacker," *Decision Analysis*, vol. 19, no. 2, pp. 99–122, 2022.

[3] H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, and S. Shetty, "Simulation for cybersecurity: state of the art and future directions," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab005, 2021.

[4] S. Hassell, P. Beraud, A. Cruz, G. Ganga, S. Martin, J. Toennies, P. Vazquez, G. Wright, D. Gomez, F. Pietryka *et al.*, "Evaluating Network Cyber Resiliency Methods using Cyber Threat, Vulnerability and Defense Modeling and Simulation," in *MILCOM 2012-2012 IEEE Military Communications Conference*. IEEE, 2012, pp. 1–6.

[5] B. Rodrigues, M. Franco, G. Parangi, and B. Stiller, "SEConomy: a framework for the economic assessment of cybersecurity," in *Economics of Grids, Clouds, Systems, and Services: 16th International Conference, GECON 2019, Leeds, UK, September 17–19, 2019, Proceedings 16*. Springer, 2019, pp. 154–166.

[6] H. Chen, H. Cam, and S. Xu, "Quantifying Cybersecurity Effectiveness of Dynamic Network Diversity," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3804–3821, 2022.