UNIVERSIDADE DE BRASÍLIA

INSTITUTO DE EXATAS - IE

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Nome: João Lucas Pinto Vasconcelos

CPF: 054.247.581-26

Proposta de Projeto de Pesquisa

Título: Crimes Informáticos e Redes de Dados: Desafios e Soluções no Contexto de Tecnologia da Informação**.**

Linha de Pesquisa: Sistemas de Computação.

Área de Pesquisa: Banco de Dados.

1 Introdução

Com a ascensão do uso da internet e o predominante domínio das mídias sociais, a sociedade encontra-se entrelaçada com as tecnologias da informação. No entanto, essa transformação tecnológica trouxe consigo novos desafios, notadamente na forma de delitos informáticos que exploram as vulnerabilidades intrínsecas das redes de dados. O ciberespaço, que encarna o domínio das redes digitais, é o *locus* onde se desenrolam atividades culturais, econômicas e interativas, além de simbolizar um ambiente onde os usuários vivenciam experiências e formam uma comunidade virtual global, possibilitando o fluxo de informações multifacetadas e plurilinguísticas. Neste contexto, as redes de dados configuram a espinha dorsal da infraestrutura de Tecnologia da Informação contemporânea, facilitando a transmissão e o intercâmbio de informações em uma escala sem precedentes.

A noção de crimes informáticos, ou cibernéticos, abarca uma vasta gama de atividades ilícitas realizadas por meio de computadores e redes de dados. Esses delitos, que se manifestam no ambiente digital, incluem práticas como o uso de *malware*, *spyware*, *hacking*, o *phishing*, o *malware* e o *ransomware*. A complexidade das infraestruturas de TI modernas, aliada à necessidade de acesso remoto, cria pontos de entrada que podem ser explorados por criminosos informáticos. Assim, a proteção de dados emerge como um desafio crítico.

Para combater crimes informáticos, é crucial adotar medidas de segurança como *firewalls*, sistemas de detecção de intrusão, criptografia robusta e autenticação multifator. Políticas de segurança e conscientização, incluindo treinamento contínuo e políticas rigorosas de senha, são essenciais. Tecnologias emergentes, como inteligência artificial, *machine learning* e *blockchain*, são fundamentais para detectar padrões anômalos, prever ataques e manter a integridade dos dados. Assim, a proteção contra crimes informáticos demanda uma abordagem multidisciplinar e soluções eficazes.

2 Justificativa

A escolha deste tema é justificada pela necessidade premente de abordar as intricadas questões da cibersegurança na era digital, na qual a interconexão tecnológica se revela onipresente. No século XXI, as tecnologias, como celulares, computadores e redes sociais, tornaram-se indispensáveis à vida cotidiana. Essa dependência intensificou-se durante a pandemia de COVID-19, quando houve um alarmante aumento de crimes cibernéticos, incluindo pornografia infantil, invasões de sistemas e vazamentos de dados pessoais. A pesquisa sobre esses crimes é de extrema relevância técnica, uma vez que a expansão da

tecnologia e da internet transformou as redes de dados em alvos primordiais para uma ampla gama de delitos digitais, exigindo o desenvolvimento de defesas robustas e eficazes.

Socialmente, a investigação sobre crimes informáticos é crucial para a formulação e implementação de políticas e regulamentações que assegurem a segurança do ambiente digital. O entendimento das ameaças digitais contribui para a criação de leis e diretrizes que garantam a proteção de dados em um cenário dinâmico e em constante evolução. O impacto econômico e social desses crimes, que inclui a perda de confiança nas tecnologias e danos à reputação das organizações, reforça a necessidade de pesquisas contínuas e do desenvolvimento de tecnologias de defesa avançadas, visando um ambiente digital mais seguro e resiliente.

3 Objetivos

3.1 Geral

Analisar os desafios e as soluções relacionadas aos crimes informáticos e à segurança das redes de dados no contexto contemporâneo da Tecnologia da Informação, com foco na identificação de vulnerabilidades, avaliação de riscos e desenvolvimento de estratégias eficazes para a proteção e integridade dos dados.

3.2 Específicos

1. Identificar e classificar os principais tipos de crimes informáticos que afetam redes de dados, incluindo *hacking*, *phishing*, *malware e ransomware*.

2. Analisar o impacto das ameaças digitais sobre a integridade dos dados e a segurança das redes. Examinar as medidas de segurança atualmente empregadas para proteger redes de dados e dados pessoais contra ataques cibernéticos, incluindo *firewalls*, sistemas de detecção de intrusão (IDS), criptografia e autenticação multifator (MFA).

4. Investigar o papel das tecnologias emergentes, como inteligência artificial (IA), machine learning (ML) e blockchain, na detecção e mitigação de crimes informáticos.

4 Revisão de Bibliografia

Os principais estudos sobre crimes informáticos e redes de dados abordam diversos aspectos críticos e em evolução deste campo. O *Internet Security Threat Report 2020* da Symantec fornece uma visão abrangente das ameaças emergentes e das técnicas cada vez mais sofisticadas utilizadas por criminosos virtuais (SYMANTEC, 2020). O *SANS 2021 Security Awareness Report do SANS Institute* examina a eficácia das estratégias de conscientização e

treinamento em segurança cibernética, revelando lacunas na formação de usuários e a necessidade de aprimoramento contínuo das práticas de segurança (SANS INSTITUTE, 2021).

A obra seminal de *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System*, estabelece o conceito fundamental de *blockchain*, com implicações significativas para a segurança dos dados e a integridade das transações digitais (NAKAMOTO, 2008). O estudo inovador da *DeepMind, Mastering the game of Go without human knowledge*, demonstra o potencial da inteligência artificial e do aprendizado de máquina para detectar e mitigar ameaças cibernéticas com precisão sem precedentes (DEEPMIND, 2017). No campo da legislação e regulamentação, *Data Privacy Law and Regulation de Bygrave* é essencial para compreender as implicações jurídicas das ameaças digitais e as medidas necessárias para proteger os dados (BYGRAVE, 2021). O *ESET Security Awareness Training Report 2021* fornece uma análise detalhada das lacunas na conscientização e treinamento em segurança cibernética, destacando a importância de abordagens educacionais contínuas para mitigar riscos (ESET, 2021).

Apesar dessas contribuições valiosas, há uma necessidade urgente de aprofundar o estudo sobre a eficácia da inteligência artificial e do *blockchain* na prevenção de crimes cibernéticos. Além disso, a aplicação prática das regulamentações de privacidade enfrenta desafios significativos, exigindo uma análise mais detalhada das políticas públicas e suas implicações para a proteção de dados em um ambiente digital em constante evolução.

5 Metodologia

A metodologia desta pesquisa será mista, integrando métodos qualitativos e quantitativos. A abordagem qualitativa incluirá análise detalhada dos crimes informáticos e suas interações com redes de dados por meio de estudos de caso e entrevistas com especialistas. Paralelamente, a abordagem quantitativa coletará e analisará dados empíricos sobre a frequência e a eficácia das medidas de segurança, bem como o impacto de tecnologias emergentes como inteligência artificial e *blockchain*. A pesquisa será teórica e descritiva, apoiada em uma revisão bibliográfica extensa e análise de dados para compreender e abordar os desafios da segurança cibernética no contexto das redes de dados.

6 Plano de Trabalho

O projeto de pesquisa iniciará com a assentimento do tema e objetivos, bem como, a revisão do plano com o orientador e elaboração do protocolo metodológico. Seguirá com a revisão bibliográfica, coleta de dados, redação dos capítulos introdutórios, revisão de literatura,

metodologia, análise de dados, resultados e discussão. Após a redação, serão realizados revisão crítica, edição e inclusão de referências conforme a ABNT. A preparação para a defesa pública incluirá a criação de slides e discurso. Após ajustes baseados no *feedback* da banca, a dissertação será submetida e defendida, com a conclusão do projeto incluindo a implementação das correções e entrega dos documentos finais ao PPGI. O objetivo é produzir uma dissertação que ofereça novas soluções para a segurança cibernética de acordo com a linha de pesquisa.

7 Cronograma

Atividades	**1º Sem.**	**2º Sem.**	**3º Sem.**	**4º Sem.**
Disciplinas obrigatórias				
Disciplinas Opcionais				
Revisão de literatura				
Definição de modelo				
Escrita da Dissertação				
Escrita de artigos científicos				
Validação em cenários propostos				
Finalização do projeto e Defesa				

8 Referências

DEEPMIND. **Mastering the game of Go without human knowledge**. Nature, v. 550, p. 354-359, 2017. DOI: 10.1038/nature24270.

BAUMAN, Sheri. **Cyberbullying and online harassment**. IN: Cowie e Myers (orgs). Cyberbullying and Online Harms. 2023.

BYGRAVE, L. A. **Data Privacy Law and Regulation**. Oxford University Press, 2021. Oxford: Oxford University Press.

ESET. **ESET Security Awareness Training Report 2021**. ESET, 2021. Disponível em: https://www.eset.com/global/research/security-awareness-training-report/. Acesso em: 27 jul. 2024.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System. 2008**. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 27 jul. 2024.

SANS INSTITUTE. **SANS 2021 Security Awareness Report. SANS Institute, 2021**. Disponível em: https://www.sans.org/security-awareness-training/2021-report. Acesso em: 27 jul. 2024.

SYMANTEC. **Internet Security Threat Report 2020**. Symantec, 2020. Disponível em: https://www.broadcom.com/company/newsroom/press-releases?filtr=latest. Acesso em: 27 jul. 2024.