Tópicos para ajudar a escolher o tema do TCC:

1. **Instalação, Configuração, Suporte e Manutenção de Computadores**: Aborda os processos de instalação, configuração, suporte técnico e manutenção de computadores.

2. **Aplicativos em Geral**: Word, Excel, Powerpoint, Photoshop, CorelDraw etc.: Explora o uso e aplicação de diversos aplicativos, como processadores de texto, planilhas, programas de apresentação e ferramentas de edição gráfica.

3. **Sistemas Operacionais e Redes de Computadores**: Cliente e Servidor: Estuda sistemas operacionais e arquiteturas de rede, abrangendo aspectos de clientes e servidores.

4. **Desenvolvimento de Sistemas (FrontEnd e ou BackEnd)**: Desktop; Dispositivos Móveis; Web; Mistos: Explora o desenvolvimento de sistemas para diferentes plataformas, como computadores desktop, dispositivos móveis, aplicações web e soluções híbridas.

5. **Suporte a usuários**: Help Desk - Aborda o atendimento e suporte técnico aos usuários, focando na resolução de problemas e assistência em TI.

6. **Inteligência Artificial e Chat GPT**: Explora a Inteligência Artificial, com ênfase em sistemas de conversação avançados, como Chat GPT (Processamento de Linguagem Natural).

7. **Sistemas de Tecnologia da Informação e Comunicação para análise de dados e suporte a tomada de decisões**: Estuda sistemas de TI e comunicação para análise de dados e apoio à tomada de decisões em empresas.

8. **Segurança Digital**: Aspectos Físicos, Aspectos Tecnológicos, Aspectos Humano: Investigação sobre a segurança de sistemas, abordando aspectos físicos, tecnológicos e fatores humanos.

9. **Computação em Nuvem**: Explora o uso e as implicações da computação em nuvem nas empresas.

10. **Internet das Coisas (IoT)**: Exploração dos dispositivos inteligentes e sensores conectados que interagem e coletam dados para melhorar processos e criar soluções inovadoras.

11. **Realidade Virtual e Aumentada**: Investigação sobre aplicações de realidade virtual e aumentada em diversos setores.

12. **E-commerce e Negócios Digitais**: Estudo de estratégias e tecnologias para impulsionar o comércio eletrônico e os negócios digitais.

13. **Análise de Big Data**: Exploração de técnicas e ferramentas para análise de grandes volumes de dados e sua aplicação na tomada de decisões e previsões.

14. **Ciência de Dados e Aprendizado de Máquina**: Investigação sobre algoritmos de aprendizado de máquina e técnicas de ciência de dados para resolver problemas complexos e realizar análises preditivas.

15. **Desenvolvimento de Jogos**: Estudo dos aspectos do desenvolvimento de jogos, incluindo design, programação, arte e narrativa.

16. **Robótica**: Exploração das aplicações da robótica em diversas áreas, como medicina, indústria, educação e serviços.

17. **Interação Humano-Computador (IHC)**: Estudo da melhoria da usabilidade e experiência do usuário em interfaces de sistemas e aplicativos.

18. **Outros tópicos:** em aberto

Dicas básicas para selecionar o Tema para o TCC:

- **Interesse e afinidade**: Primeiro, identifique dentre os tópicos aquele que mais desperta seu interesse e com o qual você se sente mais à vontade. Escolher um tema que você tenha afinidade tornará todo o processo de pesquisa e desenvolvimento mais prazeroso e motivador.
- **Relevância e aplicabilidade**: Verifique a relevância do tema no contexto atual da área de informática e sua aplicabilidade. Procure temas que tenham conexão com o mercado de trabalho ou que possam contribuir para a resolução de problemas reais.
- **Adequação ao curso técnico**: Considere se o tema escolhido está alinhado com o currículo e objetivos do curso técnico em informática. Certifique-se de que ele possa ser tratado dentro do escopo do curso e que você possua as habilidades e conhecimentos necessários para desenvolvê-lo.
- **Disponibilidade de recursos**: Verifique se há disponibilidade de recursos, como acesso a equipamentos, softwares e literatura, para conduzir a pesquisa e desenvolvimento do tema escolhido.
- **Consulte orientadores ou professores**: Compartilhe suas ideias com seus orientadores ou professores. Eles podem fornecer insights valiosos, sugerir ajustes ou até mesmo oferecer outras perspectivas que possam enriquecer o tema escolhido.
- **Viabilidade e escopo**: Certifique-se de que o tema escolhido tenha um escopo viável para o período de desenvolvimento do TCC. Evite temas muito amplos ou complexos que possam dificultar a conclusão do trabalho.

Por exemplo, se você tem interesse em análise de dados e tomada de decisões, poderia escolher o tema ***"Utilização do Power BI para Suporte à Tomada de Decisões em um Consultório de Odontologia na cidade de Casa Branca"***. Dessa forma, você estaria unindo seu interesse em análise de dados com um contexto específico e aplicação real na área de odontologia da cidade de Casa Branca.

Ao seguir essas etapas e considerar suas preferências e habilidades, você estará mais bem preparado para escolher um tema relevante e adequado para o seu TCC no curso técnico de informática.

TRABALHO DE PESQUISA

CONSIDERAÇÕES GERAIS:

O Projeto de Pesquisa é basicamente um plano de ação. Nele, você propõe uma investigação, um trabalho, algo que será formalmente organizado. Assim, o projeto serve para persuadir alguém – um leitor, um professor, um orientador – de que o que você deseja fazer é possível e valioso.

Para convencer alguém de que seu trabalho é viável, você precisa de uma base sólida. Primeiramente, isso envolve a teoria que sustenta seu trabalho. Em seguida, você precisa mostrar como será possível realizar essa ideia na prática. Por fim, é importante demonstrar o impacto que seu trabalho pode ter na área em que se insere.

Normalmente, espera-se que os projetos resultem em algo concreto, uma realização real, em vez de serem apenas formalidades. Na verdade, um projeto deve guiar e justificar o trabalho a ser feito e mostrar:

1. DE ONDE SURGE O TRABALHO:

Toda pesquisa parte de um conhecimento prévio. Suas ideias não aparecem do nada. Elas têm origens, sejam nas necessidades da área de estudo ou em teorias que sustentam essas ideias. Isso é essencial para fundamentar seu projeto. Você deve construir seu trabalho com base em teorias sólidas. Por exemplo, quais são os fundamentos por trás de uma técnica? De onde vêm as ideias para uma metodologia? Quais são os motivos racionais para usar um protocolo? Em resumo, por que seu trabalho é possível? Porque tem uma base sólida de conhecimento que o sustenta. Todo trabalho tem raízes em conhecimento anterior, que deve ser bem estabelecido e cuidadosamente entendido. Uma vez que você deixou isso claro, é hora de justificar seu trabalho.

2. POR QUE FAZER ESPECIFICAMENTE O TRABALHO:

Agora que você esclareceu a origem do seu trabalho, precisa explicar por que escolheu essa abordagem específica e não outra. Você deve justificar suas escolhas. Muitas vezes, há várias maneiras de abordar um problema, ou talvez outras técnicas já estejam sendo usadas. Sua justificativa deve mostrar por que sua abordagem é melhor. Além disso, explique os benefícios e vantagens de suas escolhas. Agora, com essas duas partes fundamentais em mente, você pode começar a planejar a estrutura do seu trabalho.

ESTRUTURANDO O TRABALHO:

A estrutura do projeto segue um guia específico, como as normas ABNT NBR 15287:2011. Embora haja variações dependendo da área do projeto, alguns elementos são comuns. Vamos dar uma olhada neles:

Título:

O título identifica o assunto principal da pesquisa. Ele deve ser claro e específico, indicando o que você irá estudar.

Introdução:

Nesta seção, você apresenta seu projeto, Defina o objeto de estudo e explique o escopo do trabalho. Quais são os limites do seu estudo?

Justificativa:

Aqui, você explica a importância do seu trabalho. Como ele contribuirá para a área de pesquisa? Por que é viável? Quais desafios podem surgir?

Objetivos:

Quais são os resultados que você espera alcançar? Quais são os objetivos gerais e específicos do seu trabalho?

Revisão da Literatura/Referencial Teórico:

Resuma as pesquisas anteriores sobre o assunto. Destaque os pontos em comum e as divergências entre os autores.

Procedimentos:

Descreva como você realizará a pesquisa. Quais materiais, métodos e etapas serão usados? Isso é essencial para que os leitores compreendam o processo.

Cronograma:

Planeje o tempo necessário para cada etapa da pesquisa. Isso mostra que você é organizado e realista em relação ao tempo disponível.

Referências:

Liste as fontes que você consultou até agora. Isso revela como você construiu suas bases de conhecimento.

EXEMPLO FICTÍCIO:

Título: Análise de Vulnerabilidades em Redes de Computadores em um Ambiente Corporativo

Introdução:

A crescente dependência de sistemas de tecnologia da informação em ambientes corporativos exige uma atenção constante à segurança das redes de computadores. Nesse contexto, a identificação e correção de vulnerabilidades são fundamentais para garantir a integridade, confidencialidade e disponibilidade dos dados. Este projeto tem como objetivo realizar uma análise de vulnerabilidades em uma rede de computadores de uma empresa fictícia, a fim de identificar potenciais ameaças e propor medidas de mitigação.

Justificativa:

A segurança da informação é uma preocupação crítica em qualquer organização que utilize sistemas de TI. A exposição a ameaças cibernéticas pode resultar em perdas financeiras, danos à reputação e violações de privacidade. A análise de vulnerabilidades desempenha um papel crucial na identificação de possíveis pontos fracos que podem ser explorados por invasores. Portanto, este estudo visa contribuir para a compreensão das principais vulnerabilidades presentes em redes de computadores corporativas e fornecer insights para aprimorar a postura de segurança.

Objetivos:

Objetivo Geral:

- Realizar uma análise de vulnerabilidades na rede de computadores da empresa fictícia "TechSecure" e propor medidas de correção e mitigação.

Objetivos Específicos:

- Identificar os principais ativos de TI da empresa, incluindo servidores, estações de trabalho e dispositivos de rede.
- Realizar uma avaliação de vulnerabilidades utilizando ferramentas de análise automatizada.
- Classificar as vulnerabilidades identificadas com base em sua gravidade e potencial impacto.
- Propor soluções e recomendações para corrigir as vulnerabilidades, priorizando medidas de segurança mais críticas.

- Elaborar um relatório detalhado das vulnerabilidades identificadas e das ações corretivas recomendadas.

Revisão da Literatura/Referencial Teórico:

A revisão da literatura constitui um alicerce fundamental deste estudo, proporcionando uma compreensão mais aprofundada dos conceitos e princípios subjacentes à segurança de redes de computadores, vulnerabilidades, ataques cibernéticos e os métodos empregados na análise de vulnerabilidades. Esta seção se baseará em uma análise criteriosa de pesquisas anteriores que abordam os desafios reais enfrentados pelas empresas em termos de segurança cibernética, bem como as abordagens recomendadas para reforçar a proteção de ambientes corporativos contra potenciais invasões.

Segurança de Redes de Computadores:

- A segurança de redes de computadores é um aspecto crítico em um cenário onde a troca de informações sensíveis e confidenciais ocorre constantemente. Estudos como o de Anderson (2015) destacam que a vulnerabilidade das redes corporativas decorre não apenas de ataques externos, mas também de ameaças internas, enfatizando a necessidade de medidas abrangentes de defesa. Exemplos de práticas de segurança, como a segmentação de redes, a implementação de firewalls e a autenticação de dois fatores, têm demonstrado sucesso na prevenção de acessos não autorizados (Doe & Smith, 2018).

Vulnerabilidades e Ataques Cibernéticos:

- A identificação de vulnerabilidades é crucial para evitar que ameaças cibernéticas explorem fraquezas nos sistemas. Estudos como o de Brown (2019) elucidam que vulnerabilidades de software, como falhas de codificação e configurações incorretas, frequentemente levam a brechas de segurança. Um exemplo notório é o ataque WannaCry, que explorou uma vulnerabilidade não corrigida no protocolo SMB da Microsoft, resultando em danos substanciais (Jones et al., 2017). Além disso, ataques de engenharia social, como phishing, demonstram como as vulnerabilidades humanas podem ser exploradas para comprometer a segurança (Johnson, 2020).

Métodos de Análise de Vulnerabilidades:

- A análise de vulnerabilidades é uma abordagem sistemática para identificar pontos fracos nos sistemas. A abordagem de avaliação automatizada, exemplificada pela ferramenta Nessus, realiza varreduras de rede para identificar configurações inadequadas e

vulnerabilidades conhecidas (Smith & Williams, 2016). A análise manual, por outro lado, envolve inspeções detalhadas de códigos e configurações, destacando vulnerabilidades específicas de aplicativos (Brown & Johnson, 2018). Estudos como o de White (2022) enfatizam a importância de abordagens híbridas que combinam avaliações automatizadas e revisões manuais para uma cobertura abrangente.

Melhores Práticas para Fortalecer a Segurança Corporativa:

- A literatura ressalta a necessidade de abordagens abrangentes para fortalecer a segurança em ambientes corporativos. A aplicação rigorosa de políticas de segurança, como o princípio do menor privilégio, pode limitar a exposição a ataques (Smith et al., 2019). Adicionalmente, a constante atualização e aplicação de patches, como evidenciado no caso do ataque Equifax (2017), demonstra a importância de manter as infraestruturas atualizadas para evitar vulnerabilidades conhecidas (Doe & White, 2020). A implementação de treinamentos de conscientização de segurança também é destacada, pois ajuda a mitigar vulnerabilidades humanas, como o compartilhamento inadvertido de informações confidenciais (Johnson & Brown, 2021).

Procedimentos:

- Levantamento de informações sobre a infraestrutura de TI da "TechSecure".
- Utilização de ferramentas de análise de vulnerabilidades, como scanners de rede e avaliadores de segurança.
- Classificação das vulnerabilidades de acordo com a gravidade e potencial impacto.
- Elaboração de um plano de ação para correção das vulnerabilidades identificadas.
- Criação de um relatório detalhado contendo resultados da análise e recomendações.

Cronograma:

O projeto será desenvolvido ao longo de 6 meses, divididos da seguinte forma:

- **Mês 1 e 2**: Levantamento de Informações e Identificação de Ativos
  - **Semanas 1-4**: Coleta de dados sobre a rede e sistemas.
  - **Semanas 5-8**: Identificação e catalogação de ativos e recursos.
  - **Resultado Esperado**: Um inventário completo de ativos e informações relevantes.
- **Mês 3**: Análise de Vulnerabilidades e Classificação de Riscos
  - **Semanas 9-12**: Realização de testes de segurança e varreduras de vulnerabilidade.
  - **Semanas 13-16**: Avaliação dos resultados dos testes e classificação de riscos.
  - **Resultado Esperado**: Lista de vulnerabilidades identificadas e sua classificação por nível de risco.
- **Mês 4 e 5**: Proposição de Medidas de Correção e Mitigação
  - **Semanas 17-20**: Desenvolvimento de estratégias para mitigar as vulnerabilidades identificadas.
  - **Semanas 21-24**: Implementação das medidas de correção e ajustes nos sistemas.
  - **Resultado Esperado**: Plano detalhado de ações para abordar as vulnerabilidades, com algumas medidas já implementadas.
- **Mês 6**: Elaboração do Relatório Final e Apresentação dos Resultados
  - **Semanas 25-28**: Documentação de todas as etapas do projeto, incluindo resultados de testes e medidas implementadas.
  - **Semanas 29-30**: Preparação da apresentação dos resultados.
  - **Resultado Esperado**: Relatório completo e coerente sobre o projeto, pronto para ser apresentado.

Referências:

- Anderson, J. (2015). Security Engineering: A Guide to Building Dependable Distributed Systems.
- Brown, M. (2019). Vulnerability Management.
- Doe, A., & Smith, B. (2018). Network Security Best Practices for Enterprises.
- Jones, C., et al. (2017). WannaCry: The Anatomy of a Ransomware Attack.
- Johnson, E. (2020). Social Engineering in the Modern Cyber Threat Landscape.
- Smith, R., & Williams, L. (2016). Automated Vulnerability Assessment Tools: A Comparative Study.
- White, S. (2022). Hybrid Approaches to Vulnerability Analysis in Network Security.