O documento apresenta uma base promissora, especialmente na atualização das referências e na tentativa de correlacionar fatores comportamentais com arquiteturas de defesa (MITRE ATT&CK, NIST e protocolos de autenticação). Contudo, como se trata de um trabalho elaborado por cinco alunos, nota-se claramente uma **"colcha de retalhos"** textual, com mudanças bruscas de estilo, dessincronia no sumário e uma queda acentuada de rigor técnico justamente na seção mais importante para um curso de Sistemas de Informação: a **Metodologia**.
Abaixo está a análise crítica detalhada e o plano de ação estruturado para você repassar ao grupo na próxima orientação.

# 1. Análise Crítica do Documento Atual

## Pontos Fortes

- **Recorte Teórico Atualizado:** As subseções **3.3.3 (Cadeia Técnica de Comprometimento)**, **3.3.4 (Mecanismos Técnicos de Mitigação)** e **3.4 (IA Generativa aplicada à Engenharia Social)** estão muito bem escritas. Elas trazem exatamente o tom esperado de um curso superior de tecnologia, referenciando frameworks de mercado (Cyber Kill Chain, MITRE ATT&CK T1566/T1204), protocolos (SPF, DKIM, DMARC, FIDO2/WebAuthn), arquitetura Zero Trust (NIST SP 800-207) e estudos recentes sobre clonagem de voz.
- **Boa articulação socio-técnica:** O uso dos princípios de persuasão de Cialdini aplicados diretamente à anatomia de templates de *phishing* (Seção 3.3.2) conecta bem a psicologia à superfície de ataque.

## Problemas Estruturais e de Formatação (Básicos, mas graves)

- **Identidade do Curso Errada na Capa:** Você mencionou que o grupo é do Bacharelado em **Sistemas de Informação**, mas na folha de rosto e na folha de aprovação consta *"obtenção do título de graduação em Ciência da Computação"*.
- **Sumário Dessincronizado:** O sumário lista tópicos que não existem ou mudaram de lugar no corpo do texto (ex.: lista *"3.2 Vulnerabilidade de configuração"*, *"3.3 Vulnerabilidade de Software"* e *"3.6 Exemplos Notórios"*, mas no texto o capítulo 3 pula de *3.1 Conceitos* direto para *3.2 Engenharia Social* e *3.3 Phishing*). Foi feito manualmente ou nunca foi atualizado no Word.
- **Deslize Conceitual no Abertura do Capítulo 3:** Na introdução do Capítulo 3, o texto diz que apresentará *"leis e normas relacionadas à segurança do trabalho"*. O correto é **Segurança da Informação** (Cibersegurança), não Segurança do Trabalho (EPIs, CIPA, etc.).
- **Citação de Fontes Secundárias de Baixo Rigor:** Na seção 3.2.3, dados da IBM, Verizon e FBI são citados através de um blog/portal secundário (DCiber, 2023), enquanto na lista de referências os relatórios originais da IBM, Verizon e FBI já estão listados. Eles devem citar a fonte primária diretamente no texto. Além disso, as referências finais não estão em ordem alfabética (padrão ABNT).
- **Gráficos sem Adaptação e sem Citação no Texto:** A Figura 1 está em inglês e com resolução baixa; a Figura 2 tem fonte sem data ou autor formal no padrão ABNT, e

nenhuma das duas é explicitamente chamada e discutida nos parágrafos que as antecedem.

### Problemas de Conteúdo e Metodologia (O Ponto Crítico)

- **O "Questionário" (Capítulo X):** O aluno deixou a dúvida no título: *(OBS: ESTE TRECHO FOI ELABORADO RECENTEMENTE E NÃO TENHO CERTEZA SE MATENHO NO TRABALHO)*.
  - **Diagnóstico:** Do jeito que está, parece um texto gerado por IA ou copiado de um manual de boas práticas, mas redigido como se a empresa estudada tivesse uma maturidade de segurança impecável (com PRI testado semestralmente, EDR, revogação de tokens, análise em sandbox e *Threat Intelligence*). Se a empresa já faz tudo isso com perfeição, como um e-mail simples de sorteio conseguiu enganar a equipe na seção seguinte?
  - **Veredito sobre o Questionário: Deve ser mantido, mas reposicionado e reenquadrado.** Ele não é um capítulo solto no Referencial Teórico. Ele é o **Instrumento de Coleta de Dados Qualitativos (Entrevista Estruturada com o Gestor de TI/Segurança)**, que deve entrar na **Metodologia** (como pergunta) e nos **Resultados** (como diagnóstico do ambiente atual da empresa antes ou depois do teste prático).
- **Fragilidade Extrema da Seção 4 (Metodologia):** Enquanto a seção 3.3.4 fala em NIST e MITRE ATT&CK, a seção 4 cai para um nível de redação muito coloquial e superficial (*"uma forma bem simples de ataque é, Um Email informando sobre um sorteio..."*, *"criar a mania de sempre checar"*). Falta especificar a arquitetura do teste: qual ferramenta foi usada para o disparo e rastreamento (ex.: GoPhish, SET, plataforma comercial)? Qual foi a infraestrutura de envio? Como garantiram a ética e o cumprimento da LGPD (ex.: não coletar senhas reais, apenas registrar o clique por ID/token, autorização formal da diretoria)?
- **Ética e Sigilo Corporativo:** Eles citam o nome real de uma empresa (*DUX Company*), pretendem colocar o CNPJ real, e no questionário citam ferramentas internas específicas (*Pasqualino One* e *Synology Chat*). Expor falhas de segurança e número de funcionários vulneráveis de uma empresa real sem anonimização pode gerar problemas jurídicos sérios para os alunos e para a universidade, a menos que haja um Termo de Consentimento expresso autorizando a divulgação do nome. **A recomendação padrão é anonimizar** (ex.: *"uma empresa de médio porte do setor de nutrição e suplementação alimentar localizada no estado de São Paulo"*).

# 2. Próximos Passos para os Alunos (Roteiro de Orientação)

Você pode dividir as tarefas entre os 5 integrantes usando a tabela abaixo como meta para a próxima entrega:

| Frente de Trabalho | Ação Necessária | Onde Aplicar |
|---|---|---|

| | | |
|---|---|---|
| **1. Decisão sobre o Questionário** | Transformar o "Capítulo X" em uma **Entrevista Estruturada de Diagnóstico de Maturidade**. Mover as perguntas para um Apêndice (ou seção de Metodologia) e usar as respostas no Capítulo 5 para confrontar a ** Segurança Prescrita** (o que a TI diz que faz no questionário) com a **Segurança Real** (quantos clicaram no phishing no teste prático). | Capítulos 4 e 5 |
| **2. Reescrita da Metodologia (Rigor de SI)** | Reescrever a Seção 4 em linguagem acadêmica formal, classificando a pesquisa (estudo de caso exploratório, quanti-qualitativo) e detalhando o **ambiente experimental**: ferramenta de simulação utilizada, configuração do domínio/remetente, construção do *template* (quais gatilhos de Cialdini foram usados no voucher), métricas coletadas (enviados, abertos, cliques) e salvaguardas éticas/LGPD. | Capítulo 4 |
| **3. Anonimização dos Dados** | Remover nomes reais (*DUX Company*, *Vultus*, *Pasqualino One*) e substituir por descrições genéricas do porte e setor da | Capítulo 4 e Questionário |

| | | |
|---|---|---|
| | organização, protegendo a empresa parceira de exposição de vulnerabilidades. | |
| **4. Consolidação dos Resultados** | Preencher as lacunas [x]. Criar gráficos e tabelas cruzando os dados do teste (ex.: taxa de cliques geral, taxa de cliques por departamento se houver, tempo médio entre o envio e o primeiro clique, e se o alerta à TI em 30 minutos descrito no questionário realmente funcionou na prática). | Capítulo 5 |
| **5. Revisão de Coesão e ABNT** | Corrigir o curso na capa para **Sistemas de Informação**; trocar "segurança do trabalho" por "segurança da informação" na abertura do Cap. 3; atualizar o Sumário automático; ordenar as referências de A a Z; remover a citação indireta do *DCiber* usando direto os relatórios da IBM/Verizon; padronizar a escrita para eliminar a sensação de textos colados de autores diferentes. | Documento inteiro |

# 3. Dica de Ouro para o Capítulo 5 (Análise e Discussão)

Para que o TCC tenha um fechamento digno de nota máxima na banca, oriente os alunos a **conectar as pontas que eles mesmos criaram**:

1. No Capítulo 3, eles explicaram a **Cyber Kill Chain** e o **MITRE ATT&CK (T1566.002 - Spearphishing Link e T1204.001 - Malicious Link)**. No Capítulo 5, ao apresentar os números de quem clicou no *voucher*, eles devem mapear exatamente em qual fase da *Kill Chain* os funcionários falharam e quais controles técnicos da seção 3.3.4 (como

DMARC ou proxy web) barraram ou deveriam ter barrado a campanha.

2. Contrastar as respostas do **Questionário da TI** com o resultado do **Teste Prático**: se o questionário afirma que a empresa faz treinamentos semestrais e simulações trimestrais, a taxa de cliques no teste dos alunos foi baixa como esperado ou ainda foi alta? Essa discussão entre *política existente vs. comportamento real* é o coração do objetivo específico nº 3 que eles prometeram na introdução.

Deseja que eu elabore uma sugestão de estrutura detalhada (tópico a tópico) para os capítulos 4 (Metodologia) e 5 (Resultados) para você entregar como modelo aos alunos?