ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

DIEGO **BONATO** LANGER, Ten Cel Av

Engenharia Social: um Risco à Segurança da Informação

Rio de Janeiro
2023

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

DIEGO **BONATO** LANGER, Ten Cel Av

Engenharia Social: um Risco à Segurança da Informação

Trabalho de conclusão de curso apresentado, como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior.
Linha de Pesquisa: Poder Aeroespacial.
Orientador: Marcelo Viegas Neves Cel Esp FOT.

RESUMO

O objetivo desta pesquisa foi identificar em que medida a percepção do militar da Aeronáutica, acerca da vulnerabilidade à Engenharia Social, pode influenciar a Segurança da Informação. Considerando que o elemento humano é o mais vulnerável quando explorado por um Engenheiro Social, esta fragilidade com a Segurança da Informação pode acarretar situações indesejáveis de comprometimento de sigilo, que não podem ser desprezadas em qualquer meio, especialmente no Comando da Aeronáutica (COMAER). Assim, para atingir o objetivo esta pesquisa se valeu de uma revisão bibliográfica, em legislações do COMAER, e de uma pesquisa bibliográfica, na literatura acadêmica, com o objetivo de identificar os conceitos acerca dos temas, assim como os métodos de prevenção à Engenharia Social. Para a aferir a percepção quando a vulnerabilidade à Engenharia Social, foi utilizado um questionário. Na comparação do conteúdo das legislações com o material acadêmico, identificou-se a necessidade da atualização de legislações do COMAER. Por meio do questionário, foi identificado um grau elevado de vulnerabilidade à Engenharia Social, assim como, falta de instruções sobre o tema, conforme orientado por legislação interna. Concluiu-se que existe a necessidade de instruções no sentido de ampliar a consciência situacional acerca da segurança, aumentando assim a prevenção à Engenharia Social, assim como, de atualizar algumas legislações sobre o tema.

Palavras-chave: engenharia social; segurança da informação; engenheiro social; fragilidade do elemento humano.

ABSTRACT

The objective of this research was to identify to what extent the perception of the Air Force military, about the vulnerability to Social Engineering, can influence Information Security. Considering that the human element is the most vulnerable when exploited by a Social Engineer, this fragility with Information Security can lead to undesirable situations of compromised secrecy, which cannot be overlooked in any environment, especially in the Air Force Command (COMAER). Thus, in order to reach the objective, this research made use of a bibliographical review, in COMAER legislation, and of bibliographical research, in the academic literature, with the objective of identifying the concepts about the themes, as well as the methods of prevention of Social Engineering. A questionary as used to assess the perception of vulnerability to Social Engineering. Comparing the content of legislation with academic material, the need to update COMAER legislation was identified. Through the questionnaire, a high degree of vulnerability to Social Engineering was identified, as well as a lack of instructions on the subject, as guided by internal legislation. It was concluded that there is a need for instructions to increase situational awareness about security, thus increasing the prevention of Social Engineering, as well as to update some legislation on the subject.

Keywords: *social engineering; information security; social engineer; fragility of the human element.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CACEM	Curso Avançado de Comando e Estado-Maior
COMAER	Comando da Aeronáutica
ECEMAR	Escola de Comando e Estado Maior da Aeronáutica
FAB	Força Aérea Brasileira
FCA	Folheto do Comando da Aeronáutica
GUARNAE	Guarnição de Aeronáutica
ICA	Instrução do Comando da Aeronáutica
SINTAER	Sistema de Inteligência da Aeronáutica
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

O ser humano ao longo dos anos, com o objetivo de melhorar a sua socialização tem desenvolvido características acolhedoras, prestativas, envolvidas com gentilezas, onde trata de forma diferenciada algumas pessoas, outras nem tanto, direcionando maior afeição àqueles que parecem ter o mesmo conhecimento ou ainda se expressam da forma semelhante. Conforme Brasil (2009), algumas destas características podem levar a uma possibilidade de exploração por parte de um Engenheiro Social, segundo Mitinick e Simon (2003) este é a pessoa que combina "a inclinação para enganar as pessoas com os talentos de influência e persuasão".

A engenharia social segundo Mitinick e Simon (2003) é a capacidade de "fazer com que as pessoas façam coisas que normalmente não fariam". Nesta perspectiva, qualquer pessoa, sem a preocupação de poder ser enganada, está sujeita a ser alvo de Engenharia Social. Ou ainda, por mais que esteja preparada, se desconhecer as novas capacidades e os novos métodos de ataques, também corre o mesmo risco. Segundo DCiber (2023) a engenharia social é "Manipulação psicológica que um criminoso pratica contra uma pessoa para que ela realize ações ou lhe forneça dados confidenciais, incluindo informações pessoais, senhas ou credenciais eletrônicas.", traduz-se assim nas palavras de Mitinick e Simon (2003) que a Engenharia Social é uma das ameaças mais eficientes a segurança da informação.

Considerando que o militar também está inserido na sociedade e, por mais que diferenciem-se possuindo características ímpares, ainda possui o seu lado humano que desfruta ao lado de seus familiares no seu cotidiano. Faz-se mister recordar que o militar também está sujeito aos mesmos riscos. Desta forma, ao identificar a perspectiva expressa na visão de futuro da Concepção Estratégica – Força Aérea 100 (BRASIL, 2018), quando em 2041 a Força Aérea completará cem anos, identifica-se que para atingir esta visão o fator humano não pode ser desconsiderado, relevante atenção deve ser dispensada aos cuidados e preocupações que este leva para a caserna.

Neste contexto, compreendendo o potencial que a engenharia social tem de atuar sobre pessoas para obter informações, cabe aqui a proposta desta pesquisa e que leva a elaboração do seguinte Problema: em que medida a percepção do militar da aeronáutica, acerca da vulnerabilidade à Engenharia Social, pode influenciar a Segurança da Informação?

De forma a responder a este problema, foi identificado um bom rumo a trilhar ao conduzir a pesquisa pelas seguintes Questões Norteadoras:

QN1) Quais são as legislações na FAB que norteiam o entendimento sobre os riscos à Segurança da Informação diante da Engenharia Social e Segurança da Informação e quais são as suas orientações para aumentar a segurança?

QN2) Quais são as legislações e orientações gerais no meio científico sobre a Segurança da Informação aplicada aos riscos da Engenharia Social e quais são as suas orientações gerais?

QN3) Como está a percepção do militar da FAB com relação à sua vulnerabilidade diante de mecanismos de engenharia social?

Assim, por meio deste caminho o Objetivo Geral desta pesquisa foi identificar em que medida a percepção do militar da Aeronáutica, acerca da vulnerabilidade à Engenharia Social, pode influenciar a Segurança da Informação. Para chegar a este objetivo geral foram elaborados os seguintes Objetivos Específicos:

OE1) Identificar as legislações da FAB que norteiam o entendimento sobre os riscos à Segurança da Informação diante da Engenharia Social e Segurança da Informação e quais são as suas orientações para aumentar a segurança;

OE2) Identificar as legislações e orientações gerais no meio científico sobre a Segurança da Informação aplicada aos riscos da Engenharia Social e quais são as suas orientações gerais;

OE3) Verificar se o compêndio de legislações castrense está em sintonia com os conhecimentos científicos; e,

OE4) Aferir o nível de percepção a vulnerabilidade a Engenharia Social, diante da necessidade de manter a Segurança da Informação.

Assim esta pesquisa busca identificar a evolução das características sociais humanas visando a melhoria da interação com outras pessoas. No entanto, essas características também podem ser exploradas por engenheiros sociais, que combinam a capacidade de enganar as pessoas com habilidades capazes de influenciar e persuadir. A Engenharia Social é a habilidade de fazer com que as pessoas ajam de maneiras incomuns, representando uma ameaça eficiente à segurança da informação. Isso também afeta os militares, que, mesmo possuindo características diferentes, estão sujeitos aos mesmos riscos no ambiente civil. A pesquisa propõe investigar a percepção dos militares da Aeronáutica em relação à vulnerabilidade à engenharia social. Para isso, foi proposta análise em legislações em busca de orientações relacionadas à Engenharia Social, bem como métodos de como identificar a percepção dos militares sobre sua vulnerabilidade. Os objetivos da pesquisa incluem revisão e pesquisa bibliográfica e verificação da sintonia entre as legislações militares e os conhecimentos científicos, além de avaliar a percepção dos militares por meio de questionário.

2 REFERENCIAL TEÓRICO

De acordo com Mitnick e Simon (2003) Engenharia Social é a arte de “fazer com que as pessoas façam coisas que normalmente não fariam para um estranho”. De forma análoga e ajustada à terminologia militar, adequada ao COMAER, a FCA 200-3 (Prevenção a Engenharia Social) em suas conceituações vai mais além definindo Engenharia Social como “o processo de enganar (manipular) pessoas de forma que elas forneçam diretamente ou proporcionem acesso à informação privada, classificada ou privilegiada a alguém que não deveria tê-la” (BRASIL, 2009).

Compreendendo que a Engenharia Social “se concentra em explorar as fraquezas das pessoas, dos sistemas de Tecnologia da Informação (TI) e dos processos de segurança de TI” (BRASIL, 2009) entende-se que o problema da segurança está no elemento de TI e no elemento humano. Contudo, na visão de Mann (2011) quando indaga “quem é o responsável pela Segurança da Informação?”, o autor apresenta três figuras em resposta, sugerindo que a segurança humana seria um elo perdido entre a segurança em TI e a segurança física. Neste sentido é interessante lançar um olhar sobre a evolução em termos de segurança nos aspectos citados por Mann.

Com relação a segurança física, desde os primórdios o homem compreendeu a necessidade e importância em proteger os seus bens de interesse. Desta forma, os conceitos da necessidade de possuir uma segurança adequada estão muito alicerçados no seu entendimento.

Com relação a segurança em TI, cabe destacar que o meio cibernético é bastante recente a exploração de suas potencialidades de uso, assim como dos seus riscos, são novos e evoluem com grande rapidez. Desta forma, a esta corrida entre novidades tecnológicas e as novidades dos riscos é algo muito presente e debatido na atualidade. Se por um lado, como Dias (2021) evidencia que a vantagem competitiva aliada à facilidade e adaptabilidade na gestão de informação crítica para os negócios, por outro o crime cibernético tem evoluído com as mesmas características. Assim é possível compreender que a busca pela segurança em TI já é uma constante, talvez não em todos ambientes por questões de priorização, mas sempre acompanha a evolução de TI.

Recorrendo a ideia formada por Mitnick e Simon (2003) onde mostram que com o aumento da preocupação com segurança que pretende minimizar as vulnerabilidades técnicas, os atacantes voltam-se cada vez mais para o elemento humano, visto que, normalmente, é mais fácil, não exige custos elevados e possui riscos mínimos. Assim pode-se identificar onde reside a importância do elo perdido citado por Mann (2011): no elemento humano.

Confirmando esta questão da fragilidade do elemento humano diante dos demais recursos de TI que envolvem o meio cibernético, DCiber (2023) cita o aumento em 37% de ataques cibernéticos no terceiro trimestre de 2022, como forma de prevenir são destacadas 8 ameaças e suas orientações de prevenção, dentre as ameaças está a Engenharia Social.

A fragilidade humana está ligada a diversos fatores, segundo Mann (2011) envolve a ignorância, a credulidade, a facilidade e a obediência. Para Mitnick e Simon (2003) a relação com a ingenuidade ligada ao desconhecimento de boas práticas relacionadas à segurança. A ABNT (2013) cita apenas a presença de vulnerabilidades inerentes ao elemento humano. Já Brasil (2009) destaca a tendência natural das pessoas em serem prestativas e possíveis de seres sugestionadas por diversos gatilhos psicológicos. De uma forma geral, os autores entendem que muitas vezes as pessoas desconhecem o verdadeiro valor da informação que possuem, gerando assim a negligência sobre o elemento humano. Então passa a ser um fator primordial dedicar atenção a este aspecto da segurança, especialmente com relação a segurança da informação.

Com esta preocupação, a ABNT (2013) destaca que a segurança da informação pode ter a vulnerabilidade ampliada devido a fatores internos e externos, sendo que uma forma de evitar isso é por meio da implementação de controles, políticas, processos, estruturas organizacionais.

Assim, com a definição de Engenharia Social como a arte de fazer com que as pessoas ajam de forma incomum e forneçam informações privadas a desconhecidos. A Segurança da Informação é afetada tanto pelo elemento tecnológico quanto pelo elemento humano. A pesquisa destaca a importância do elo perdido entre a segurança em TI e a segurança física, que é a segurança humana. Enquanto a segurança física tem sido compreendida desde os primórdios, a segurança em TI é mais recente e está em constante evolução, mas a fragilidade do elemento humano é explorada, sendo a Engenharia Social a principal ameaça. A pesquisa ressalta que as pessoas muitas vezes desconhecem o valor das informações que possuem e podem ser influenciadas por gatilhos psicológicos. Portanto, é fundamental dedicar atenção ao fator humano na Segurança da Informação, implementando controles e políticas adequadas.

Considerando os conceitos apresentados, esta pesquisa debruçou-se sobre a importância do fator humano, não apenas no aspecto organizacional, de controles, políticas e processos, mas também recorrendo ao meio cibernético, onde atualmente, estão mergulhados todos os meios de comunicação, redes sociais, serviços e muitos outros.

2.1 Entendendo um ataque de Engenharia Social

Segundo Tetri e Vourinen (2013) é possível entender um ataque de engenharia social quando o problema é analisado de forma multidimensional. Na visão dos autores estas dimensões seriam: coleta de dados, persuasão e fabricação.

A *coleta de dados,* normalmente, ocorre antes do ataque e é o momento em que o Engenheiro Social identifica as informações que mais facilmente permitirá acessar sua vítima ou seu alvo. Para efetivar uma coleta de dados as ações são as mais variadas, tais como uma busca no lixo, uma por busca em redes sociais ou pesquisas na Internet, muitas vezes, chegando a interação com pessoas próximas ao alvo. Nas palavras de Souza e Fernandes (2016) o aumento do uso de sistemas de comunicação digital tem tornado complexo o cenário de confiança interpessoal, ocasião em que muitos se aproveitam da complexidade crescente que gera oportunidade de obtenção fácil de dados.

A *persuasão* é o momento é que o engenheiro usa dos gatilhos psicológicos para ganhar a confiança das pessoas. Os métodos utilizados envolvem manipulação do estado emocional, por meio da sobrecarga, reciprocidade, autoridade entre outros (BRASIL, 2009). A persuasão trabalha com o convencimento da pessoa alvo de que o Engenheiro Social é alguém que está ali para auxiliar.

A *fabricação* envolve ações que legitimam a interpretação do papel que o Engenheiro Social está representando, variando desde mensagens e a forma de expressão técnica, chegando até a utilização de símbolos, uniformes, credenciais e jargões relacionados com o ambiente do ataque.

Considerando que vulnerabilidade pode ser definida como uma “propriedade intrínseca de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência” (ISO, 2009), para o elemento humano a vulnerabilidade está associada ao risco. Recorrendo a definição de risco da ISO (2009), é possível entender risco como o “efeito da incerteza sobre o objetivo”. Neste aspecto a incerteza, permite identificar muitas vezes por meio da percepção humana as chances de uma ocorrência negativa ou positiva, levando o indivíduo a criar uma percepção de segurança. Assim compreende-se que a percepção de segurança está diretamente relacionada a percepção de vulnerabilidade do indivíduo.

Sob esta análise, Viana (2017) desenvolveu uma pesquisa baseada no modelo multidimensional apresentado por Tetri e Vourinem (2013). Neste estudo foi validado um instrumento de pesquisa que utilizou o modelo desenvolvido por Ratchford e Banhart (2012) para avaliar a percepção de vulnerabilidade de um público alvo.

Neste sentido, esta pesquisa apropriou-se do trabalho de Viana (2017) para avaliar a percepção de vulnerabilidade dos militares FAB diante da Engenharia Social de forma a quantificar esta vulnerabilidade.

De acordo com Tetri e Vourinen (2013), um ataque de engenharia social pode ser compreendido através de três dimensões: coleta de dados, persuasão e fabricação. A coleta de dados ocorre antes do ataque, onde o engenheiro social identifica informações que facilitarão o acesso à vítima. A persuasão envolve o uso de gatilhos psicológicos para ganhar a confiança da pessoa, enquanto a fabricação consiste em ações que legitimam o papel desempenhado pelo engenheiro social. A vulnerabilidade do elemento humano está associada ao risco, sendo que a percepção de segurança está diretamente relacionada à percepção de vulnerabilidade. Viana (2017) desenvolveu uma pesquisa para avaliar a percepção de vulnerabilidade com base em um modelo multidimensional, e a presente pesquisa utiliza esse trabalho para quantificar a percepção de vulnerabilidade dos militares da FAB diante da engenharia social.

3 METOTOLOGIA

Para atingir os objetivos desta pesquisa utilizou-se uma abordagem quantitativa, visto que foi realizado um levantamento em um grupo significativo de pessoas, onde foram obtidas conclusões correspondentes aos dados coletados (Gil, 2023). A pesquisa foi ainda do tipo descritiva pois tinha o propósito de avaliar condições de variáveis na população específica, que por sua vez se aproximou-se de uma pesquisa exploratória uma vez que conduziu a uma nova visão da importância da fragilidade fator humano diante da Engenharia Social (Gil, 2023).

Na pesquisa foram utilizados como variáveis de comparação, informações comuns aos militares, que permitiram distinguir características socioeconômicas para isso foi usado como fator comparativo a variação de posto ou graduação, de vínculo profissional, de tempo de serviço associado à idade e de gênero. Como forma de ampliar as observações, foram analisadas ainda as 3 dimensões apresentadas por Tetri e Vourinen (2013), assim como os fatores de influência utilizados na elaboração dos questionamentos.

Com objetivo de descortinar conceitos, técnicas e métodos acerca da relação entre Engenharia Social e Segurança da Informação, na busca de atingir uma solução para o OE1, foi desenvolvida uma revisão bibliográfica em documentos do COMAER. Assim como foi realizada uma pesquisa bibliográfica na área acadêmica ligada aos temas para expandir os conceitos acerca dos temas, com a intenção de atingir uma solução ao OE2.

Para atingir o OE3 foram identificados os assuntos que as legislações do COMAER apresentavam carência.

Por fim, foi utilizado um instrumento de pesquisa que tinha por finalidade contribuir para o atingimento do OE4. Este instrumento foi adaptado da pesquisa de Viana (2017), para as condições adequadas ao COMAER.

O referido questionário foi composto de 26 questões distribuídas em 3 partes. Na primeira parte havia 6 questões que tinham por objetivo caracterizar as variáveis socioeconômicas dos respondentes. Sendo 1 de seleção de informação (posto ou graduação), outras 2 fechadas (gênero e vínculo profissional) e outras 3 de informação descritiva (idade, tempo de serviço e OM).

A parte do questionário que foi adaptado de Viana (2017) era composta por 16 questões em escala de Likert de 5 pontos (1 a 5), onde 1 representou discordo totalmente e 5 concordo totalmente. Estas 16 questões foram distribuídas em 3 categorias de análises selecionadas, que guardam relação direta com as 3 dimensões (coleta de dados, fabricação e persuasão) apresentadas Tetri e Vourinen (2013) na sua pesquisa. O objetivo destas questões era identificar a percepção de vulnerabilidade a Engenharia Social. É importante destacar que a resposta mais próxima da concordância com a afirmativa apresentada nas questões aponta para possível fragilidade a engenharia social, enquanto a discordância indica uma maior resistência.

Por fim, para aderência do questionário a conhecimentos disponíveis no COMAER, para a população específica, foram criadas 4 questões fechadas, sendo 3 de forma dicotômica e 1 com 4 opções.

Devido a limitação de tempo para a pesquisa, associado ao fato de o questionário ser uma adaptação de Viana (2017), entendendo que o mesmo já foi aplicado, optou-se por não realizar o pré-teste no questionário.

O questionário está disponível no Apêndice A, para distribuição o mesmo foi adaptado a ferramenta *Google Forms* e distribuído por meio do e-mail corporativo da FAB. Para atingir a uma variação significativa que permitiria distinguir características socioeconômicas foi utilizado o efetivo militar de algumas das OMs da GUARNAE-AF. O universo populacional calculado foi de 1970 militares.

Foram identificados alguns fatores limitantes da pesquisa, dentre eles: 1) a pouca disponibilidade de tempo para a realização da pesquisa; 2) a dificuldade na seleção do corpo amostral que apresentasse uma maior variedade socioeconômico acessível ao tempo disponível para a pesquisa; e, 3) a reduzida adesão ao questionário, que foi identificado, além do curto

prazo de tempo disponibilizado para a aplicação do mesmo, como decorrente do próprio receio do respondedor em entrar em um *phishing*[1].

Nesta pesquisa, foi utilizada uma abordagem quantitativa, por meio de um levantamento realizado em um grupo significativo de pessoas, visando obter conclusões correspondentes aos dados coletados. A pesquisa foi descritiva e exploratória, buscando avaliar condições de variáveis em uma população específica e fornecer uma nova visão da importância da fragilidade do fator humano diante da Engenharia Social. Foram utilizadas variáveis socioeconômicas como critérios de comparação, além das três dimensões apresentadas por Tetri e Vourinen (2013) e fatores de influência na elaboração dos questionários. Uma revisão e uma pesquisa bibliográfica foram realizadas para obter conceitos, técnicas e métodos relacionados à Engenharia Social. Foi adaptado um instrumento de pesquisa com o objetivo de contribuir para o alcance dos objetivos estabelecidos. O questionário foi aplicado através do e-mail corporativo da FAB em um grupo de militares selecionados. Foram identificados fatores limitantes, como a falta de tempo, dificuldade na seleção da amostra e baixa adesão devido ao receio de *phishing*.

4 APRESENTAÇÃO DE DADOS E ANÁLISE DE RESULTADOS

O trabalho inicial baseou-se em uma revisão bibliográfica em documentos do COMAER para identificar conceitos e procedimentos já contidos nos documentos que atuem no sentido de proteger o efetivo da Engenharia Social. Em um momento posterior houve uma pesquisa bibliográfica sobre o referido tema.

Por fim, para avaliar a percepção da vulnerabilidade a Engenharia Social foi aplicado um instrumento de pesquisa no formato de questionário.

4.1 DOCUMENTOS DO COMAER

Na revisão bibliográfica foi identificada como a principal publicação na área a FCA 200-3 Prevenção a Engenharia Social que traz conceitos, princípios e gatilhos por onde o engenheiro social pode atuar para convencer a vítima de realizar a ação desejada. A publicação sugere a aplicação de uma defesa multinível cujo objetivo é “determinar quais são as vulnerabilidades e ameaças e armar as defesas contra elas” (Brasil, 2009).

---

[1] Técnica que utiliza simula uma solicitação de dados legitima para roubas os dados pessoais, geralmente utilizada na internet como um site. Exemplos de dados roubados: login e senha de acesso, dados pessoais, senha de banco.

A defesa multinível propõe, inicialmente, a criação e divulgação de Política de Segurança, não só em nível de TI, mas de forma ampla. Em seguida sugere o processo de treinamento de consciência de segurança que permita a todos entenderem quais assuntos possuem importância e devem ser tratados com sigilo, citando ainda os principais gatilhos por onde a engenharia social pode ser aplicada. O pessoal que atua em posições-chaves precisa de um reforço com um treinamento de resistência. Devem haver lembretes contínuos do risco da Engenharia Social. A partir deste ponto é sugeria a aplicação de minas antiengenharia social. Para tal seriam criados fluxos que devem passar obrigatoriamente por pontos de alta segurança, de forma que caso ocorra uma tentativa de ação ela vai esbarrar na mina e com isso o engenheiro será exposto. Por fim, a defesa multinível sugere que exista um processo bem definido de quem e como é acionado caso seja identificada uma ação anormal.

Foi identificado que a FCA 200-2 Mentalidade de Segurança foi uma publicação criada antes da FCA 200-3 (BRASIL, 2009). Na publicação são encontrados exemplos de informações que podem requerer maior preocupação ou sigilo, assim como o tipo de perfil de pessoas que podem querer explorar estas informações. Traz uma visão inicial do que seria a Engenharia Social, assim como formas de ataque e alvos. Descreve sucintamente o motivo do porquê podem ocorrer falhas na segurança, inclusive em meio a TI. Por fim, traz algumas medidas preventivas de forma bastante superficial.

Já a ICA 200-11Programa Básico de Trabalho Anual e Educação Continuada dos Elos do SINTAER sugere um roteiro geral para os elos do SINTAER (Brasil, 2013), neste roteiro estabelece a necessidade de uma aula com dois tempos de 45 a 50 minutos, com periodicidade semestral, para o público interno da OM para trabalhar com o assunto da FCA 200-3 (BRASIL, 2009). Assim como outra aula com a mesma duração, periodicidade e público alvo para trabalhar com o conteúdo da FCA 200-2

Durante a revisão bibliográfica, foi identificado como principal publicação na área a FCA 200-3 Prevenção a Engenharia Social, que aborda conceitos, princípios e gatilhos utilizados pelos engenheiros sociais para convencer as vítimas a realizar ações desejadas. Essa publicação sugere a aplicação de uma defesa multinível, que envolve a criação de políticas de segurança, treinamento de conscientização, treinamento de resistência para posições-chave, implementação de minas antiengenharia social e estabelecimento de processos para lidar com ações anormais. Além disso, foi identificado que a FCA 200-2 Mentalidade de Segurança fornece exemplos de informações que requerem sigilo, tipos de perfis de pessoas que podem explorar essas informações e medidas preventivas. A ICA 200-11 Programa Básico de Trabalho

Anual e Educação Continuada dos Elos do SINTAER (BRASIL, 2013) sugere a inclusão de aulas sobre as publicações FCA 200-3 e FCA 200-2 no programa de treinamento interno.

Esta parte da pesquisa levou a ser atingido o OE1, ao identificar as legislações da FAB que norteiam o entendimento sobre os riscos à Segurança da Informação diante da Engenharia Social e Segurança da Informação e quais são as suas orientações para aumentar a segurança.

4.2 PUBLICAÇÕES ACADÊMICAS

Foram identificados diversos conceitos já apresentados ao longo de todo este artigo. A lógica de como ocorre a Engenharia Social é sempre a mesma, o que muda ao longo do tempo são as novas formas de como ela é aplicada. Sem nunca esquecer que os métodos mais antigos sempre voltam a ser aplicados.

No livro de Mitnick e Simon (2003) são apresentadas técnicas com o uso de telefone, o uso de uniformes e de credenciais, diálogo direto com a vítima, entre outros. Com o advento e uso constante de redes sociais a fonte de informações sobre possíveis alvos aumentou de forma significativa. Pinto e Berenguel (2020) trazem a informação de vetores de ataques no meio virtual como formas de coleta de dados e ataque. Dias (2021) mostra formas de prevenção ao *phishing*.

No trabalho de Meier (2018) relata ataque que utiliza ferramentas de comunicação instantânea (WhatsApp ou SMS), meio de comunicação que com a Pandemia do COVID-19 ganhou grande evidência e uso generalizado.

Nesta parte da pesquisa, foram identificados diversos conceitos relacionados à engenharia social, que já foram apresentados ao longo do artigo. A lógica do funcionamento da engenharia social permanece a mesma, mas as formas de aplicação estão em constante evolução, embora os métodos mais antigos também sejam retomados. O livro de Mitnick e Simon (2003) descreve técnicas como o uso do telefone, uniformes, credenciais e diálogo direto com a vítima. Com o crescimento das redes sociais, houve um aumento significativo da disponibilidade de informações sobre possíveis alvos. Pinto e Berenguel (2020) discutem vetores de ataques no ambiente virtual, enquanto Dias (2021) aborda formas de prevenção contra *phishing*. Meier (2018) relata um ataque que utiliza ferramentas de comunicação instantânea, como o WhatsApp ou SMS, que ganharam destaque e ampla utilização durante a pandemia do COVID-19.

É notório que a literatura sobre o tema Engenharia Social não se limita àquelas aqui apresentadas, contudo, entendeu-se que o objetivo para esta pesquisa, especialmente, para

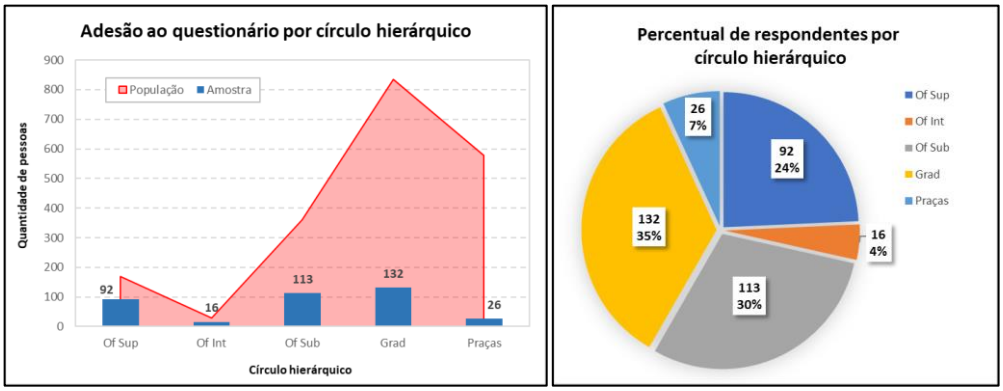
atingir o OE2, as obras pesquisadas foram o suficiente. Com isso, o OE2 foi atingido ao identificar as legislações e orientações gerais no meio científico sobre a Segurança da Informação aplicada aos riscos da Engenharia Social e quais são as suas orientações gerais.

4.3 DADOS DO QUESTIONÁRIO

O questionário foi encaminhado a OMs da GUARNAE-AF, utilizando os grupos pré-definidos de efetivo da OM. A amostra populacional selecionada para a pesquisa era composta de 1970 militares com o número de respondentes de 386 pessoas. Dos respondentes uma das pessoas informou que pertencia a uma OM que não havia sido selecionada para a pesquisa e outras 6 pessoas que eram civis, em vista do foco da pesquisa foram considerados 379 respondentes. Segundo Parker e Rea (2000) seria necessária uma amostra de 323 para população de 2000 pessoas para ter um nível de confiança de 95% com desvio padrão de 5%. Para o caso da pesquisa, considerando a população de 1970 e o tamanho da amostra de 379, com um nível de confiança de 95% a margem de erro foi 4,53%.

As 6 questões iniciais focavam na identificação do perfil do respondente, levando em consideração a informação relativo ao Posto/Graduação. Foi possível identificar que a adesão por círculo hierárquico comparado com a população de cada círculo ocorreu da seguinte forma: 92 oficiais superiores representando 54,44% de adesão, 16 oficiais intermediários representando 57,14% de adesão, 113 oficiais subalternos representando 31,39% de adesão, 132 graduados representando 16,07% de adesão e 26 praças representando 4,50% de adesão. Conforme disponível no Gráfico 1.

Gráfico 1 - Gráficos Adesão ao Questionário por Círculo Hierárquico (E) e Percentual de Respondentes por Círculo Hierárquico Considerando a Amostra(D).

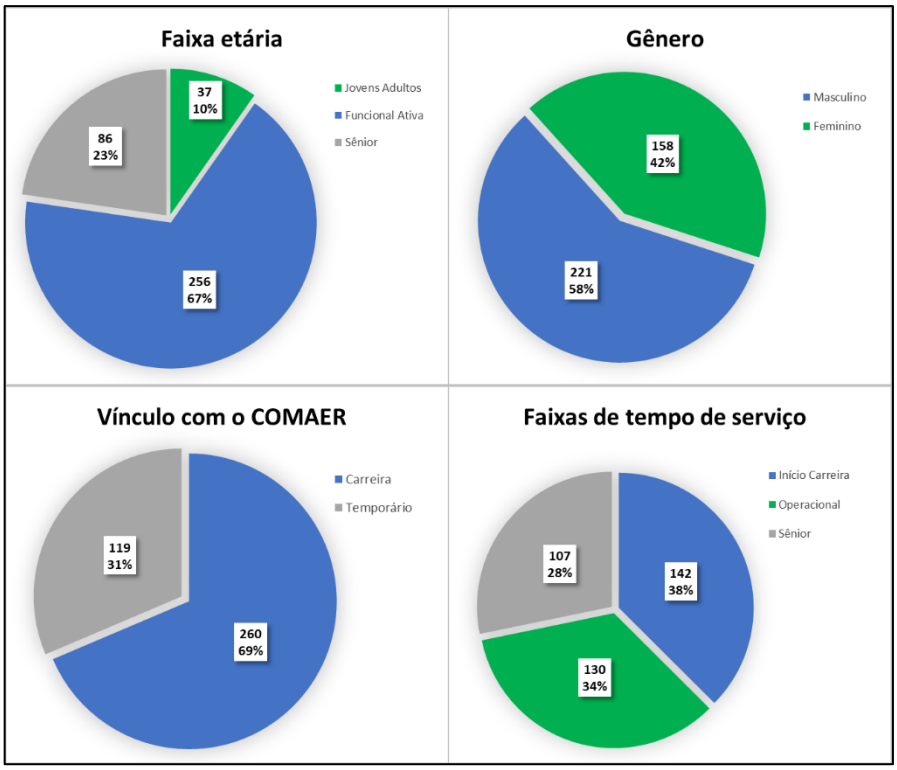


Fonte: O Autor

Com relação ao gênero as respostas foram: 221 masculino e 158 feminino. Com relação ao vínculo profissional as respostas foram: 260 militares de carreira e 119 temporários. Com

relação a faixa etária foram estabelecidos 3 grupos, sendo eles: jovem adulto (até 30 anos), funcional ativa (de 30 anos a 45 anos) e sênior (acima de 45 anos). Nas faixas etárias as respostas foram: 37 de jovem adulto, 256 de funcional ativa e 86 de sênior. Com relação ao tempo de serviço também foram estabelecidas 3 faixas, sendo elas: início carreira (até 10 anos), operacional (de 10 a 25 anos) e sênior (acima de 25 anos). Nestes grupos de tempo de serviço os respondentes estão distribuídos da seguinte forma: 142 no início de carreira, 130 no grupo operacional e 107 como sênior. Estes dados podem ser observados no Gráfico 2.

Gráfico 2- Distribuição das Respostas Conforme as Variáveis de Comparação



Fonte: O Autor

Nas questões de 7 a 22, que compreendem a adaptação do questionário de Viana (2017), as respostas foram distribuídas conforme a sua temática. A correlação entre a questão e o domínio e a temática é possível identificar no Apêndice B. Na Tabela 1 é possível verificar a média encontrada nas questões de 7 a 22, com o mapeamento das dimensões segundo Tetri e Vuorinen (2013).

Tabela 1 - Médias das questões

DIMENSÃO	**MÉDIA DAS RESPOSTAS**					
PERSUASÃO	3,87	2,68	2,84	1,87	3,22	2,98
FABRICAÇÃO	3,36	2,66	2,14	1,67	2,02	-
COLETA DE DADOS	1,76	1,55	4,29	3,6	2,18	-

Fonte: O Autor

No Apêndice C é possível verificar a média das respostas separadas pelas variáveis analisadas, sendo elas: círculo hierárquico, vínculo com o COMAER, grupo etário, grupo de tempo de serviço e gênero. Na Tabela 2 abaixo é possível identificar a média de cada dimensão.

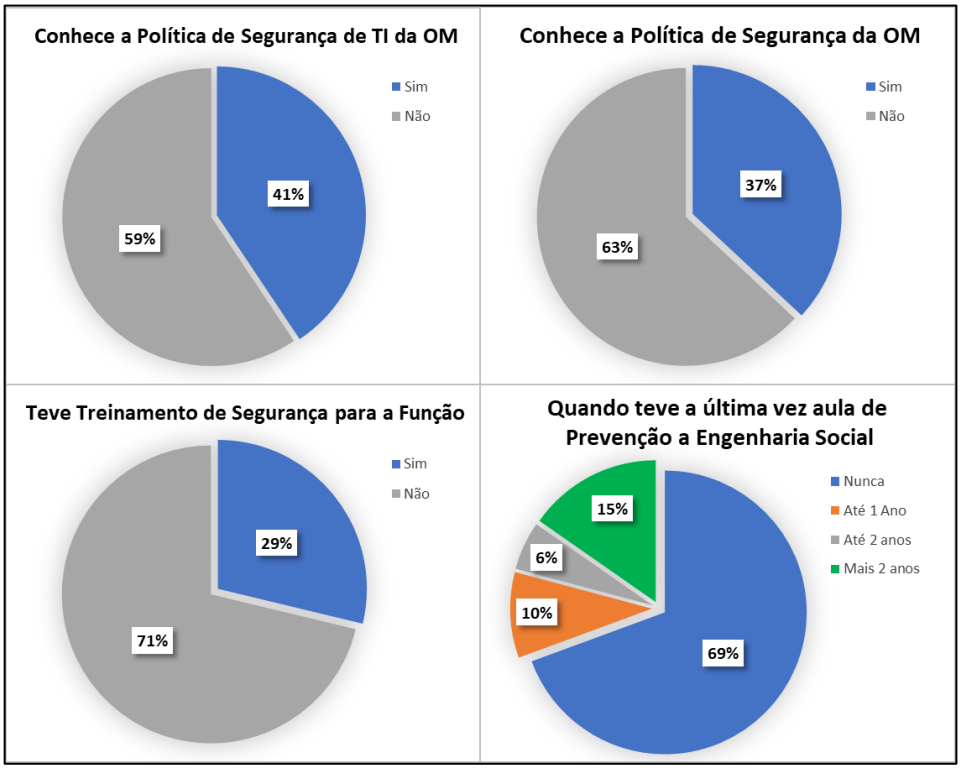
Tabela 2 - Média das dimensões

DIMENSÃO	PERSUASÃO	COLETA DE DADOS	FABRICAÇÃO
MÉDIA	2,91	2,68	2,37

Fonte: O Autor

Na parte das questões de 23 a 26 sobre conhecimentos de prevenção as respostas foram como segue. Na questão 23, sobre o conhecimento da política de TI da OM, 154 informaram que conhecem e 228 desconhecem. Na questão 24, sobre a política de segurança da OM, 140 informaram que conhecem e 242 que desconhecem. Na questão 25, sobre ter tido treinamento de segurança para a função que ocupa, 110 responderam que tiveram orientações e 272 responderam que não tiveram. Na questão 26, sobre o treinamento de prevenção a Engenharia Social, 265 responderam que nunca tiveram, 38 que tiveram a menos de 1 ano, 21 que tiveram a menos de 2 anos e 58 que tiveram a mais de 2 anos. Estes dados podem ser observados no Gráfico 3.

Gráfico 3 - Respostas Referente as Perguntas Específicas ao COMAER



Fonte: O Autor

Nesta parte da pesquisa, um questionário foi enviado para OMs da GUARNAE-AF, com uma população de 1970 militares. Foram obtidas respostas de 386 pessoas, incluindo uma

pessoa de uma OM não selecionada e 6 civis, resultando em 379 respondentes considerados relevantes. A amostra atendeu aos critérios estatísticos estabelecidos por Parker e Rea (2000) para um nível de confiança de 95% e margem de erro de 4,53%. As questões iniciais do questionário buscaram identificar o perfil dos respondentes, revelando a adesão por círculo hierárquico: 92 oficiais superiores, 16 oficiais intermediários, 113 oficiais subalternos, 132 graduados e 26 praças. Quanto ao gênero, foram 221 masculino e 158 feminino, e em relação ao vínculo profissional, 260 eram militares de carreira e 119 temporários. Faixas etárias e tempo de serviço também foram considerados. As questões de 7 a 22, adaptadas de Viana (2017), abordaram diferentes temas, e a média das respostas foi mapeada em dimensões específicas. As questões de 23 a 26 investigaram o conhecimento dos respondentes sobre políticas e treinamentos de segurança, revelando os níveis de familiaridade.

4.4 ANÁLISE DOS DADOS

Em uma breve análise temporal entre o período das últimas edições das legislações avaliadas, é possível identificar uma evolução nos conceitos de prevenção acerca dos danos causados pela Engenharia Social. A FCA 200-2 (BRASIL, 2008) apresenta uma ideia superficial mostrando os riscos, principais alvos e meios de ataques da engenharia social, passando para a FCA 200-3 (BRASIL, 2009), que já é uma publicação dedicada exclusivamente ao tema, analisando princípios, gatilhos e sugerindo um meio de prevenção por meio de treinamento. Finalizando, a ICA 200-11 (BRASIL, 2013) atribui aos elos do SINTAER a responsabilidade de semestralmente apresentar ao efetivo sob sua responsabilidade aulas sobre os temas Mentalidade de Segurança e Prevenção a Engenharia Social.

Contudo, é importante observar que na última década a Engenharia Social passou por uma evolução nos meios de ação, passando a ter relevância maior no meio cibernético. Quer seja por meio de redes sociais, ou mesmo por meio de sistemas, aplicativos ou soluções que a falta de conhecimento do usuário aumenta a sua exposição. Esta observação é possível ser constatada pela evolução dos meios de ataque apresentados nos trabalhos de Pinto e Berenguel (2020) e de Dias (2021), por exemplo.

A pandemia do COVID-19, que isolou em suas residências uma camada significativa da população mundial, propiciou um aumento significativo em golpes que evitam o contato humano e utilizam o meio cibernético, visto que no período pandêmico as distâncias se dilataram e o contato físico era evitado.

Com isso observa-se a necessidade da revisão de publicações como a FCA 200-3 de forma a elevar o nível de consciência do efetivo para os novos meios de ataques, que na época da sua edição, eram incipientes. Outro item que requer um destaque na revisão da publicação é o uso funcional generalizado de ferramentas computacionais de troca de mensagens instantânea, cujo banco de dados e gestão de mensagens estão a cargo de empresa privada, como por exemplo WhatsApp, Signal, Telegram, entre outros.

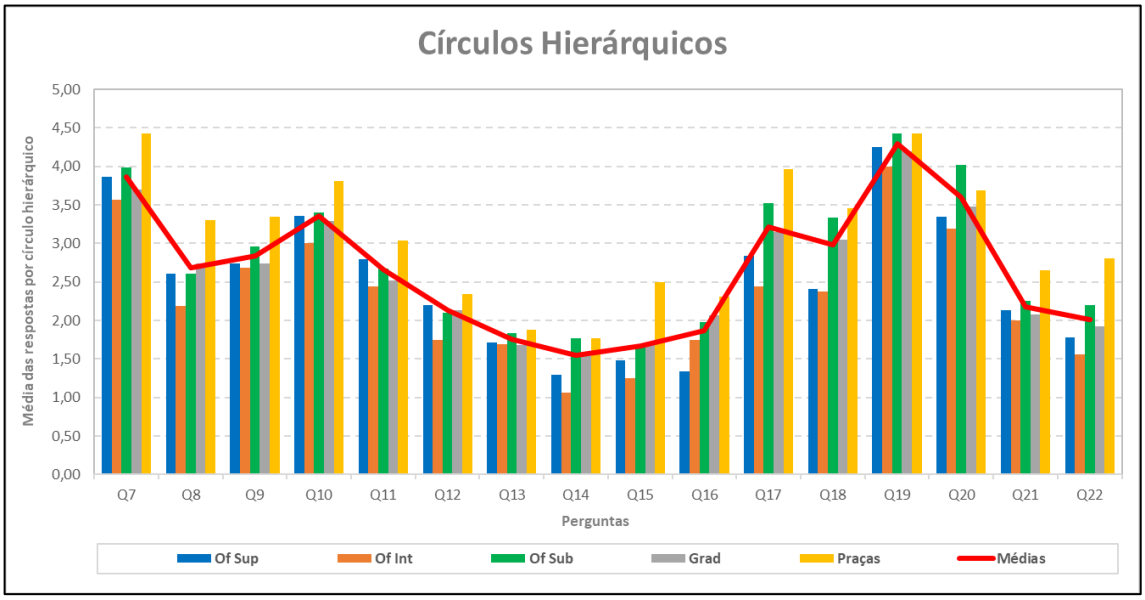
Assim, o OE3 foi atingido ao verificar se o compêndio de legislações castrense está em sintonia com os conhecimentos científicos.

As respostas apresentadas ao questionário permitem múltiplas interpretações em diversas análises. Nesta pesquisa, as análises se limitaram as tendências apresentadas na variação com a média da população para os grupos selecionados, que foram: círculo hierárquico[2], vínculo com o COMAER, gênero, grupo de faixa etária, grupo de faixa de tempo de serviço, as tendências das dimensões apresentadas por Tetri e Vuorinen (2013) e por fim a avaliação das maiores variações do questionário.

Analisando a comparação da média dos círculos hierárquicos é possível verificar uma tendência de maior vulnerabilidade apresentada nos círculos mais modernos, como o de praças e o de oficiais subalternos. Cabe destacar que no primeiro grupo poucos são de militares de carreira, apenas cabos que totalizam 15% da amostra, enquanto que no segundo grupo, muitos oficiais são temporários, totalizando 79% da amostra. Esta tendência é possível observar na Gráfico 4.

[2] Segmentação distributiva dos postos conforme segue: oficiais superiores (coronel, tenente-coronel e major), oficiais intermediários (capitão), oficial subalterno (1º e 2º tenente e aspirante), graduados (suboficiais, 1º, 2º e 3º sargento) e praças (cabo, soldado especializado e soldado).

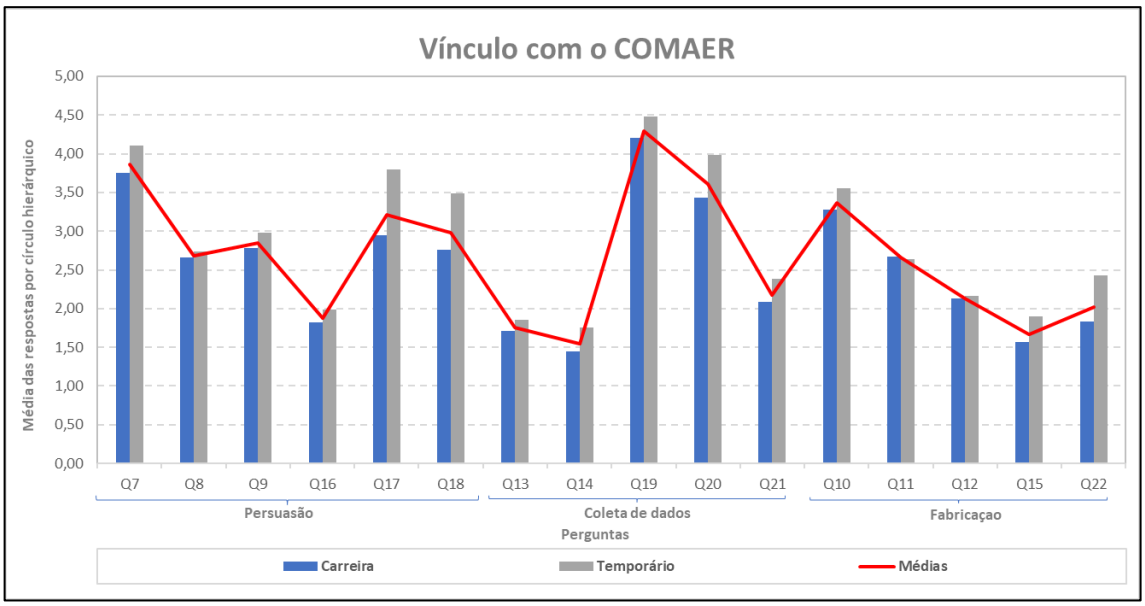
Gráfico 4 - Comparação das Médias por Círculos Hierárquicos



Fonte: O Autor

Ao analisar a comparação das médias dos respondentes que tem vínculo com o COMAER, é possível observar que entre os temporários há uma maior tendência a vulnerabilidade a engenharia social. Conforme pode ser observado na Gráfico 5.

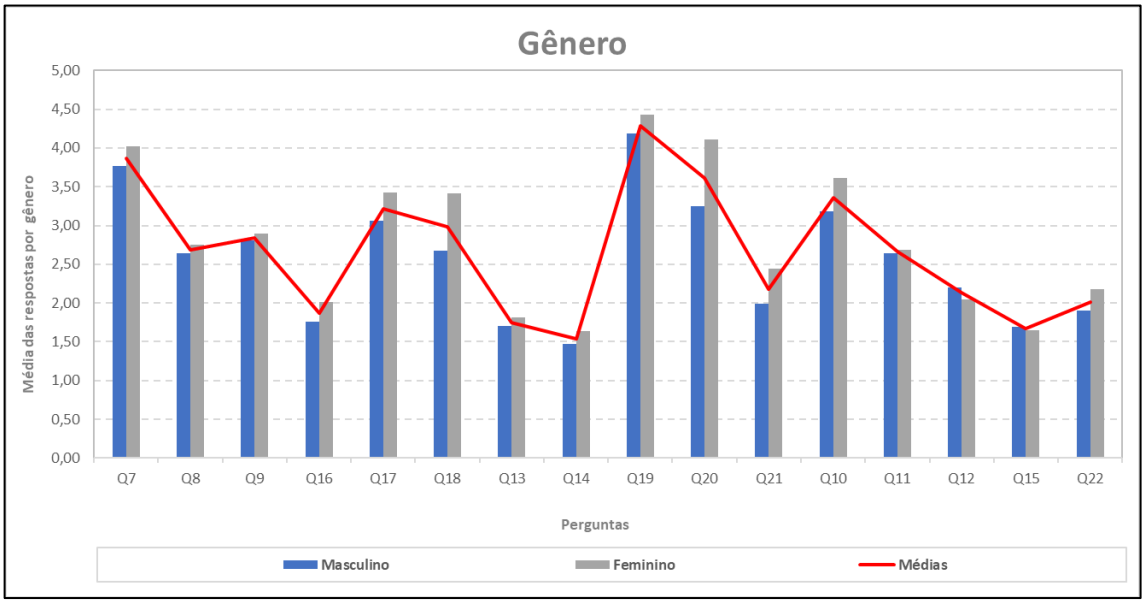
Gráfico 5 - Comparação das Médias por Vínculo com o COMAER



Fonte: O Autor

Analisando a variação das respostas usando como comparativo o gênero, identifica-se uma maior vulnerabilidade no gênero feminino, exceto na questão 12. Essa questão trabalha com a credulidade associando a aparência amigável a confiança. Estas observações podem ser verificadas no Gráfico 6.

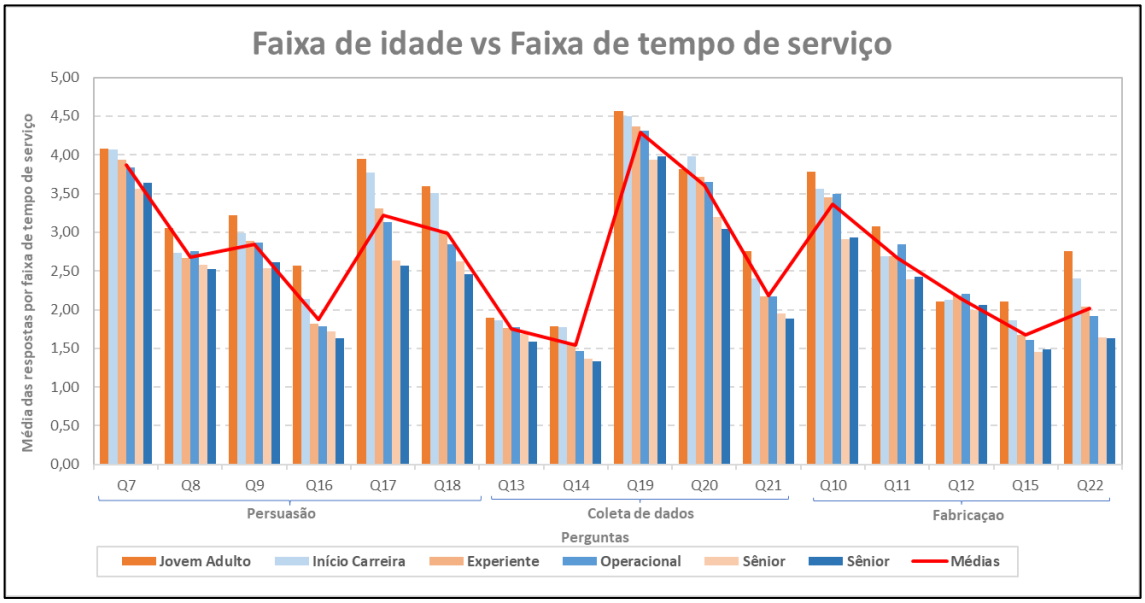
Gráfico 6 - Comparação das Médias por Gênero



Fonte: O autor

Na análise das médias das respostas comparando as faixas de idade com a faixa do tempo de serviço. Percebe-se a tendência a uma maior vulnerabilidade nas pessoas mais jovens, com leve tendência de redução da vulnerabilidade naqueles que estão no início da carreira. Esta tendência é bastante natural, considerando que oficiais temporários podem ser incorporados já em uma faixa maior de idade. Nas demais faixas etárias e tempo de serviço é possível identificar que conforme a pessoa adquire maior experiência, o seu nível de vulnerabilidade começa a reduzir. Como pode ser observado no Gráfico 7.

Gráfico 7 - Comparação das Médias por Faixas Etárias com a Faixa de Tempo de Serviço



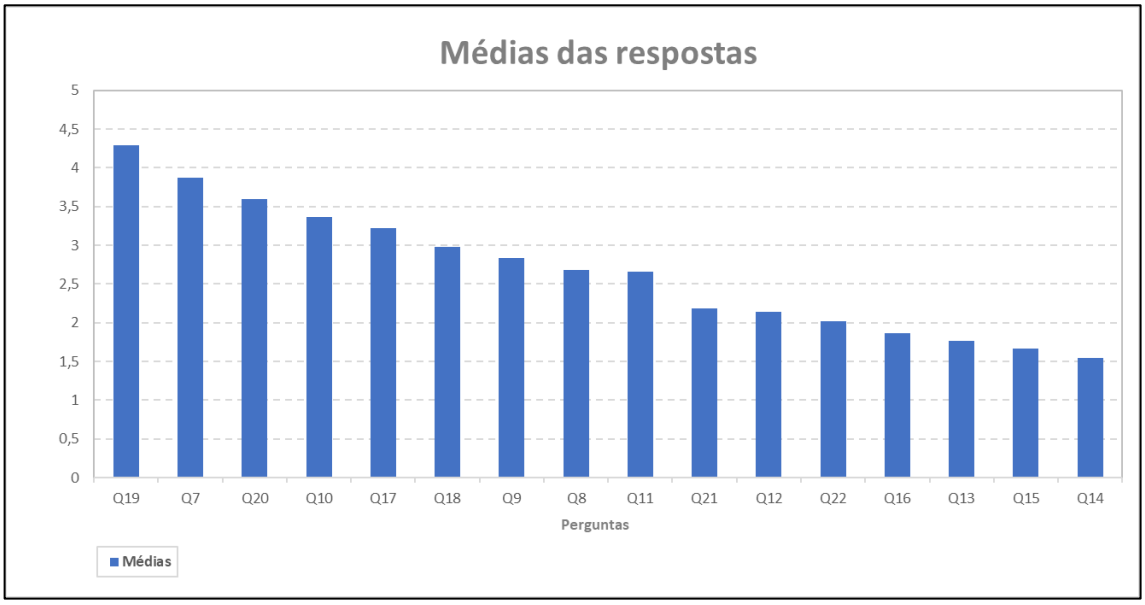
Fonte: O Autor

Conforme já verificado na Tabela 2 não houve variação significativa na comparação das médias das dimensões estudadas. A média geral da percepção de vulnerabilidade a Engenharia Social foi 2,67 com um desvio padrão de 0,27.

Com esta informação identifica-se que o OE4 foi atingido ao aferir o nível de percepção a vulnerabilidade a Engenharia Social, diante da necessidade de manter a Segurança da Informação.

Ao analisar as médias gerais, ordenadas de forma decrescente, é possível verificar quais as maiores tendências a vulnerabilidade. Como pode ser observado na Gráfico 8.

Gráfico 8 - Médias Ordenadas por Vulnerabilidade



Fonte: O Autor

Na questão 19 é possível identificar a possibilidade da coleta de dados, por meio do desconhecimento da fragilidade no uso de aplicativos de mensagens comerciais (WhatsApp, Telegram, SIGNAL, entre outros) para a comunicação no ambiente de trabalho. Isso torne urgente a abordagem de pontos como estes na documentação do COMAER que versa sobre Engenharia Social, considerando que este é um tema que atualmente não está incluso na FCA 200-3 (BRASIL, 2009).

A questão 7 utiliza a persuasão, por meio da reciprocidade. Esta área que é comum a natureza humana, conforme descrito por Mitnick e Simon (2003) está presente na grande vulnerabilidade humana. Já a temática da questão 20 utiliza da coleta de dados por meio do risco de perda de dados sensíveis com relação a estrutura de caracteres utilizados em senhas, esta problemática costuma ser difundida por diversos canais, ainda assim constitui riscos devido a fragilidade por meio da dimensão cibernética.

Por fim, em sentido de maior vulnerabilidade, é importante citar a questão 10 que mais uma vez traz aspectos relacionados com a fragilidade da natureza humana, onde alguém mal intencionado, por meio da fabricação, personificando em alguém que atraia a vítima, pode utilizar de informações falsas na troca de informações pessoais com a vítima.

No que diz respeito às preocupações sobre os riscos da Engenharia Social, foi observada uma evolução na prevenção ao longo do tempo, com publicações do COMAER abordando o tema de forma mais aprofundada. No entanto, é importante ressaltar que a Engenharia Social evoluiu, principalmente no contexto cibernético, com ataques cada vez mais direcionados a redes sociais e sistemas. A pandemia do COVID-19 também contribuiu para a mudança de cenário, levando os golpes para o meio digital devido ao distanciamento físico. Os resultados do questionário revelaram tendências de vulnerabilidade em diferentes grupos, como praças e oficiais subalternos, pessoal temporário e gênero feminino. Observou-se também uma redução da vulnerabilidade com a experiência e o tempo de serviço. Além disso, foram identificadas questões específicas de maior vulnerabilidade, como o uso de aplicativos comerciais para comunicação no ambiente de trabalho e a fragilidade da natureza humana na troca de informações pessoais.

5 CONCLUSÃO

Ao verificar a capacidade que a Engenharia Social tem de levar pessoas a fazerem algo que não desejam, inclusive disponibilizando informações sigilosas e mesmo pessoais, imaginando que estão agindo de forma correta, entende-se que este é um risco que não pode ser desprezado na gestão da segurança da FAB.

Desta forma este artigo teve como objetivo identificar em que medida a percepção do militar da aeronáutica, acerca da vulnerabilidade a Engenharia Social, pode influenciar a Segurança da Informação.

Para atingir a este objetivo, foi apresentada a relevância da fragilidade do elo humano frente a Engenharia Social, enfatizando os riscos que esta pode trazer para o COMAER.

Foram apresentados os referenciais teóricos, discorrendo sobre conceitos acerca da fragilidade do elemento humano, que segundo o consenso dos autores trata-se da parte mais frágil e onde na maior parte das vezes a segurança é menosprezada. Foi descrita a avaliação do trabalho de Tetri e Vourinen (2013) onde a Engenharia Social é analisada de uma forma multidimensional, como uma solução adotada no trabalho de Viana (2017) que desenvolveu

uma ferramenta de pesquisa para permitir a avaliação da percepção da vulnerabilidade a Engenharia Social, sendo que esta pesquisa se apropriou deste questionário.

O terceiro capítulo apresentou a metodologia que foi empregada assim como os meios e técnicas para atingir os objetivos específicos e ao objetivo da pesquisa. Foram apresentadas ainda as limitações observadas na pesquisa.

Foi identificado que os militares da FAB possuem uma distribuição bastante próxima de percepção da vulnerabilidade a Engenharia Social em cada uma das dimensões propostas por Tetri e Vourinen (2013). Com uma média de 2,91 para persuasão, 2,68 para coleta de dados e 2,37 para fabricação. Considerando a média da pesquisa, chega-se 2,67 com um desvio padrão de 0,27. Tal valor associado a informação de que 69% da amostra nunca teve uma instrução de prevenção a engenharia social, alto desconhecimento de política de Segurança da OM e alto índice de pessoas que não tiveram treinamento de segurança para a sua função, identifica-se um grau elevado de vulnerabilidade a Engenharia Social. Tais observações demandam de ação imediata com instrução do efetivo.

Em uma análise no conteúdo das questões que houveram maior vulnerabilidade, destaca-se: 1) a grande influência da natureza humana, que tem hábitos ligados a reciprocidade, conforme descrito por Mitnick e Simon (2003); 2) elevado grau de uso funcional de aplicativos de mensagem instantânea que não são controlados pelo COMAER; e, 3) uso dados conhecidos em senhas.

Assim, entende-se que o objetivo deste artigo, que foi identificar em que medida como a percepção dos militares da Aeronáutica, acerca da vulnerabilidade à Engenharia Social, pode influenciar a Segurança da Informação, foi atingido, respondendo ao problema de pesquisa. Ao identificar este nível acentuado de vulnerabilidade à Engenharia Social é possível compreender a contribuição deste artigo para a FAB, ao demonstrar a necessidade de melhorar os processos de prevenção à Engenharia Social. Visto que, como descritos por Mitinick e Simon (2003) ou Mann (2011) o elemento humano possui vulnerabilidades intrínsecas que com treinamento e atenção podem ser evitadas, sendo esta uma das ações necessárias para uma Força Aérea que deseja atingir quaisquer objetivos, criar uma estrutura forte em seu alicerce funcional, para minimizar efeitos indesejáveis.

Com relação as limitações aplicadas às conclusões obtidas neste trabalho, devido a reduzida amostra, especialmente de círculos hierárquicos de graduados e praças, convêm que as considerações encontradas sobre vulnerabilidade do militar à Engenharia Social não sejam extrapoladas para o COMAER, mas que seja considerado o alto grau de vulnerabilidade

apresentado por parte significativa dos respondentes. Cabe destacar que, as conclusões acerca da necessidade de atualização de legislação possuem grande importância.

Por fim, em vista deste estudo ter identificado grande vulnerabilidade com relação a pontos específicos como uso de produtos comerciais com caráter pessoal para serviços funcionais, como sugestão a futuros trabalhos fica a proposta de avaliações e análises de meios computacionais utilizados nesta situação, especialmente, para atividades administrativas, operacionais e que demandam sigilo. Outra sugestão para trabalhos futuros seria identificar e explorar avaliando a efetividade nas OMs da defesa multinível recomendada na FCA 200-3.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria n. 1597/GC3 de 10 de outubro de 2018. Aprova a reedição da DCA 11-45 “Concepção Estratégica – Força Aérea 100”. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 180, 15 out. 2018.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria nº 02/CIAER, de 8 de outubro de 2009. Aprova a edição do Folheto que dispõe sobre Prevenção a Engenharia. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, nº 206, p 7576-7591, de 6 de novembro de 2009.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria nº 1869/GC3, de 15 de dezembro de 2015. Aprova a Edição da Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, nº 237, p 12051-12104, de 28 de dezembro de 2015.

Catalog of Bias. **Selection Bias**. Disponível em: https://catalogofbias.org/biases/selection-bias/. Acesso em: 17 jun. 2023.

DCiber. **As 8 ameaças de cibersegurança mais comuns nas empresas e como preveni-las.** [online]. Disponível em: https://dciber.org/as-8-ameacas-de-ciberseguranca-mais-comuns-nas-empresas-e-como-preveni-las/. Acesso em: 22 jun. 2023.

DIAS, P R S. **Prevenir um Ataque de Phising**. Dissertação (Mestrado em Informática), Instituto Superior de Tecnologias Avançadas de Lisboa, Portugal, 2021

ISO – International Organization for Standardization. **ISOGUIDE 73:2009: Risk management –Vocabulary**. 2009. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en>. Acesso em: 01 maio 2023.

MANN, I. **Engenharia Social**. São Paulo: Blucher, 2011.

MEIER, L. F. M. **Engenharia social: um caso de estudo dos riscos de um ataque efetuado por um ex-funcionário**. 2018. 35 f. Trabalho de Conclusão de Curso (Especialização em Gestão da Tecnologia da Informação e Comunicação) - Universidade Tecnológica Federal do Paraná (UTFPR), Curitiba, 2018.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar. Ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Makron Books, 2003.

PARKER, A. R.; REA, L. M. **Metodologia de pesquisa: do planejamento à execução**. São Paulo: Pioneira Thomson Learning, 2002.

PINTO, L. T. S.; BERENGUEL, O. L. **Engenharia Social: A porta de entrada para informações confidenciais**. Revista Científica e-Locução, v. 1, n. 17, p. 16, 10 jul. 2020.

SOUZA, R. C. de; FERNANDES, J. H. C. **Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais.** Brazilian Journal of Information Science: research trends, *[S. l.]*, v. 10, n. 1, 2016. DOI: http://dx.doi.org/10.36311/1981-1640.2016.v10n1.08.p63 . Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/view/5088. Acesso em: 22 jun. 2023.

TETRI, P.; VUORINEN, J. **Dissecting social engineering. Behaviour & Information Technology**, v. 32, n. 10, p. 1014-1023, 2013. DOI: http://dx.doi.org/10.1080/0144929X.2013.763860.

VIANA, J. A. L. **O uso das tecnologias de informação e comunicação na terceira idade e a vulnerabilidade à engenharia social**. 2017. 107 f. Dissertação (Mestrado em Administração) – Centro de Ciências Sociais, Universidade Federal da Paraíba, João Pessoa, 2017. Disponível em: https://repositorio.ufpb.br/jspui/handle/tede/9378. Acesso em: 05 abr. 2023.

VIANA, J. A. L., ALVES, A. J. C., LIMA, P. G. S. **Vulnerabilidade à Engenharia Social: um estudo com alunos do Instituto Federal da Paraíba (IFPB)**. Revista Principia - Divulgação Científica e Tecnológica Do IFPB, 59(4), 1344, 2022. DOI: https://doi.org/10.18265/1517-0306a2021id5834.

APÊNDICE A – Questionário

O questionário aplicado foi disponibilizado na ferramenta *Google Forms* e apresentou-se da seguinte forma:

QUESTIONÁRIO DE PESQUISA:

Questionário referente à Pesquisa "Engenharia Social: Um Risco a Segurança da Informação" desenvolvida no Curso de Comando e Estado-Maior - 2023 da Escola de Comando e Estado-Maior da Aeronáutica.

APRESENTAÇÃO DO OFICIAL ALUNO:

Eu, Ten Cel AV Diego Bonato Langer, Oficial-Aluno matriculado no Curso de Comando e Estado-Maior (CCEM-2023). Estou desenvolvendo pesquisa acerca de Engenharia Social no âmbito da Força Aérea. A Engenharia Social é um método sofisticado de manipulação psicológica que representa um risco significativo à Segurança da Informação. Por meio de técnicas persuasivas e enganosas, os invasores exploram a natureza humana, persuadindo indivíduos a revelar informações confidenciais, como senhas, dados pessoais ou corporativos, e outras informações valiosas. O objetivo desta pesquisa é identificar a percepção da vulnerabilidade à Engenharia Social.

OBJETIVO DO QUESTIONÁRIO:

O objetivo deste questionário é identificar a percepção sobre a vulnerabilidade à Engenharia Social, levando em consideração as dimensões habitualmente conhecidas sobre Engenharia Social.
Informo que este questionário é anônimo e os dados somente serão utilizados para análise e processamento estatístico.
Não existem respostas certas ou erradas. Contudo é importante que seja usado o máximo de sinceridade para responder ao questionário.
Cabe aqui destacar que o objetivo do questionário não é identificar o comportamento ideal esperado, mas a ação que normalmente cada respondedor tomaria.

DISPOSIÇÃO FINAL:

Diante do exposto, ressalta-se que as informações prestadas serão destinadas exclusivamente para a conclusão do Trabalho de Conclusão de Curso (TCC) do CCEM-2023 e que os dados serão confidenciais e será mantido o anonimato dos respondentes.

IDENTIFICAÇÃO DE PERFIL:

As questões a seguir tem a finalidade de identificar o perfil da pessoa que respondeu o questionário.

Q1) Qual seu posto ou graduação?

Questão fechada que apresentou como opções de resposta uma lista suspensa com as opções:

a) Ten Brig
b) Maj Brig
c) Brig
d) Cel
e) Ten Cel
f) Maj
g) Cap
h) 1º Ten
i) 2º Ten
j) Asp
k) SO
l) 1º Sgt
m) 2º Sgt
n) 3º Sgt
o) Cb
p) S1
q) S2
r) Civil efetivo do COMAR
s) Civil sem vínculo com o COMAER.

Q2) Qual o seu vínculo profissional com o Comando da Aeronáutica?

Questão fechada que permitia a seleção de apenas uma opção com as seguintes opções:

a) Sou de carreira
b) Sou temporário
c) Não possuo Vínculo

Q3) Qual a sua idade?

Questão aberta que filtrava a possibilidade de um número entre 18 e 80.

Q4) Qual o seu gênero?

Questão fechada que permitia a seleção de apenas uma opção com as seguintes opções:

a) Masculino
b) Feminino

c) Prefiro não informar

Q5) Qual o seu tempo de serviço em anos?

Questão aberta que filtrava a possibilidade de um número entre 0 e 60.

Q6) Qual a sua OM?

Questão aberta.

QUESTÕES SOBRE RELACIONAMENTO:

Nas questões a seguir serão tratados de assuntos sobre a sua postura social no que tange a relação a com outras pessoas, independente do meio de comunicação, podendo ser pessoalmente, por meio de telefone, por aplicativo de mensagem ou mesmo pela Internet. Nas próximas questões haverá uma afirmação. Marque o quanto você discorda ou concorda com aquela afirmação em uma escala de Likert de 5 valores. Sendo os valores:
1 - Discordo totalmente
2 - Discordo
3 - Sou indiferente
4 - Concordo
5 - Concordo totalmente

Q7) Quando alguém faz uma coisa por mim, sinto que eu deveria fazer o mesmo por ele(a).

Q8) Se eu gosto de alguém, irei ajudá-lo(a) mesmo em situações em que provavelmente eu não deveria.

Q9) Eu acho importante seguir o comportamento do grupo do qual eu participo e das pessoas que eu admiro.

Q10) Quando estou em uma boa conversa com alguém, se a pessoa fala um pouco de si, acabo falando um pouco de mim também.

Q11) Eu confio nas pessoas que mostram que gostam das mesmas coisas de que eu gosto.

Q12) Pessoas que se mostram amigáveis são, normalmente, confiáveis.

QUESTÕES SOBRE O USO DE INTERNET E REDES:

Nas questões a seguir serão tratados de assuntos sobre a sua postura nas com relação ao uso de redes sociais e Internet.
Nas próximas questões haverá uma afirmação. Marque o quanto você discorda ou concorda com aquela afirmação em uma escala de Likert de 5 valores. Sendo os valores:
1 - Discordo totalmente
2 - Discordo
3 - Sou indiferente
4 - Concordo
5 - Concordo totalmente

Q13) Eu não me preocupo com os dados pessoais que eu publico nas redes sociais.

Q14) Eu publico com frequência, nas redes sociais, fotos de tudo o que eu faço, para deixar minha família e amigos informados.

Q15) Sempre que recebo mensagens ou e-mail com informações vantajosas, procuro saber mais, mesmo que precise abrir alguns arquivos que recebi junto.

QUESTÕES SOBRE A POSTURA NO AMBIENTE DE TRABALHO:

Nas questões a seguir serão tratados de assuntos sobre a sua postura com relação no ambiente de trabalho.
Nas próximas questões haverá uma afirmação. Marque o quanto você discorda ou concorda com aquela afirmação em uma escala de Likert de 5 valores. Sendo os valores:
1 - Discordo totalmente
2 - Discordo
3 - Sou indiferente
4 - Concordo
5 - Concordo totalmente

Q16) Se eu precisar de ajuda com o sistema, eu forneço a minha senha (Portal do Militar, SIGADAER, SILOMS) para alguém que demonstre pode ajudar a resolver o problema.

Q17) Eu prefiro cumprir uma ordem do que ter problemas por não cumpri-la.

Q18) Quando sou questionado por alguém que parece ser meu superior, eu sempre respondo tudo o que este alguém me pergunta.

Q19) Uso aplicativos de mensagens (WhatsApp, Telegram, Signal) para me comunicar com alguém sempre que possível.

Q20) Para não esquecer as minhas senhas, eu costumo utilizar palavras e números conhecidos que me façam lembrá-la com mais facilidade.

Q21) Para não esquecer as minhas senhas, eu costumo escrevê-las em um lugar de fácil acesso.

Q22) Quando recebo ligação ou mensagem questionando informações sobre alguém com que trabalho (telefone, local onde foi, entre outros) sempre tento ajudar como posso.

QUESTÕES SOBRE CONHECIMENTOS DE PREVENÇÃO:

Nas questões a seguir serão identificados os seus conhecimentos com relação a Segurança da Informação.
Todas as respostas a seguir são fechadas, marque a resposta que é melhor adequada a questão apresentada. Apenas uma opção pode ser marcada.

Q23) Você conhece a política de segurança de Tecnologia da Informação da sua OM? (neste documento é onde está descrito o que pode e o que não pode ser feito na rede interna e nos ativos de TI da OM).

Questão fechada que permitia a seleção de apenas uma opção com as opções Sim e Não.

Q24) Você conhece a política de Segurança de Informação da sua OM? (Neste documento devem estar descritas as informações que são sigilosas, restritas e não pode ser divulgado ostensivamente).

Questão fechada que permitia a seleção de apenas uma opção com as opções Sim e Não.

Q25) Quando você assumiu a sua função, houve treinamento ou explicação informando sobre o que era restrito, sigiloso ou ostensivo?

Questão fechada que permitia a seleção de apenas uma opção com as opções Sim e Não.

Q26) Quanto foi a última vez que você teve a instrução de Prevenção à Engenharia Social?

Questão fechada que permitia a seleção de apenas uma opção com as seguintes opções:

a) Nunca tive
b) Há menos de 1 ano
c) Há mais de 1 ano e menos que 2 anos
d) Há mais de 2 anos

APÊNDICE B – Mapeamento das questões do questionário

Tabela 3 – Mapeamento das Questões Distribuídas Pela Numeração, Dimensão e Fator de Influência

Nº	Afirmação	Dimensão	Fator
Q7	Quando alguém faz uma coisa por mim, sinto que eu deveria fazer o mesmo por ele(a).	Persuasão	Reciprocidade
Q8	Se eu gosto de alguém, irei ajudá-lo(a) mesmo em situações em que provavelmente eu não deveria.	Persuasão	Reciprocidade
Q9	Eu acho importante seguir o comportamento do grupo do qual eu participo e das pessoas que eu admiro.	Persuasão	Reciprocidade
Q10	Quando estou em uma boa conversa com alguém, se a pessoa fala um pouco de si, acabo falando um pouco de mim também.	Fabricação	Personificação do Eng. Social
Q11	Eu confio nas pessoas que mostram que gostam das mesmas coisas de que eu gosto.	Fabricação	Credulidade
Q12	Pessoas que se mostram amigáveis são, normalmente, confiáveis.	Fabricação	Credulidade
Q13	Eu não me preocupo com os dados pessoais que eu publico nas redes sociais.	Coleta de dados	Desconhecimento da fragilidade
Q14	Eu publico com frequência, nas redes sociais, fotos de tudo o que eu faço, para deixar minha família e amigos informados.	Coleta de dados	Desconhecimento da fragilidade
Q15	Sempre que recebo mensagens ou e-mail com informações vantajosas, procuro saber mais, mesmo que precise abrir alguns arquivos que recebi junto.	Fabricação	Criação de ambiente favorável
Q16	Se eu precisar de ajuda com o sistema, eu forneço a minha senha (Portal do Militar, SIGADAER, SILOMS) para alguém que demonstre pode ajudar a resolver o problema.	Persuasão	Autoridade
Q17	Eu prefiro cumprir uma ordem do que ter problemas por não cumpri-la.	Persuasão	Autoridade
Q18	Quando sou questionado por alguém que parece ser meu superior, eu sempre respondo tudo o que me perguntam.	Persuasão	Autoridade
Q19	Uso aplicativos de mensagens (WhatsApp, Telegram, Signal) para me comunicar com alguém sempre que possível.	Coleta de dados	Desconhecimento da fragilidade
Q20	Para não esquecer as minhas senhas, eu costumo utilizar palavras e números conhecidos que me façam lembrá-la com mais facilidade.	Coleta de dados	Risco a perda de dados pessoais
Q21	Para não esquecer as minhas senhas, eu costumo escrevê-las em um lugar de fácil acesso.	Coleta de dados	Risco a perda de dados pessoais
Q22	Quando recebo ligação ou mensagem questionando informações sobre alguém com que trabalho (telefone, local onde foi, entre outros) sempre tento ajudar como posso.	Fabricação	Desconhecimento do valor da informação

Fonte: o Autor

APÊNDICE C – Respostas do Questionário

Tabela 4 - Médias das respostas da dimensão Persuasão

	Domínio	**Persuasão**					
	Questão	**Q7**	**Q8**	**Q9**	**Q16**	**Q17**	**Q18**
	Médias	3,87	2,68	2,84	1,87	3,22	2,98
Círculo Hierárquico	**Of Superiores**	3,87	2,61	2,74	1,34	2,84	2,41
	Of Interm.	3,56	2,19	2,69	1,75	2,44	2,38
	Of Subalernos	3,99	2,61	2,96	1,98	3,52	3,34
	Graduados	3,70	2,73	2,73	2,07	3,15	3,05
	Praças	4,42	3,31	3,35	2,31	3,96	3,46
Vínculo	**Carreira**	3,76	2,65	2,78	1,81	2,95	2,75
	Temporário	4,11	2,75	2,98	1,99	3,79	3,48
Grupo Idade	**Sênior**	3,56	2,58	2,53	1,72	2,64	2,63
	Func. Ativa	3,95	2,66	2,89	1,82	3,30	3,01
	Jovem Adulto	4,08	3,05	3,22	2,57	3,95	3,59
Grupo Tempo de Serviço	**Sênior**	3,64	2,52	2,62	1,63	2,57	2,46
	Operacional	3,85	2,75	2,88	1,78	3,13	2,84
	Início Carreira	4,07	2,74	2,99	2,13	3,77	3,51
Gênero	**Masculino**	3,76	2,64	2,81	1,76	3,06	2,67
	Feminino	4,02	2,75	2,90	2,01	3,42	3,41

Fonte: O Autor

Tabela 5 - Médias das respostas da dimensão Fabricação

	Domínio	**Fabricação**				
	Questão	**Q10**	**Q11**	**Q12**	**Q15**	**Q22**
	Médias	3,36	2,66	2,14	1,67	2,02
Círculo Hierárquico	**Of Superiores**	3,36	2,79	2,20	1,48	1,78
	Of Interm.	3,00	2,44	1,75	1,25	1,56
	Of Subalernos	3,40	2,67	2,10	1,69	2,20
	Graduados	3,29	2,52	2,13	1,68	1,92
	Praças	3,81	3,04	2,35	2,50	2,81
Vínculo	**Carreira**	3,28	2,68	2,12	1,57	1,83
	Temporário	3,55	2,64	2,16	1,90	2,43
Grupo Idade	**Sênior**	2,91	2,40	2,00	1,45	1,64
	Func. Ativa	3,45	2,70	2,18	1,68	2,04
	Jovem Adulto	3,78	3,08	2,11	2,11	2,76
Grupo Tempo de Serviço	**Sênior**	2,93	2,42	2,07	1,49	1,63
	Operacional	3,50	2,85	2,20	1,62	1,92
	Início Carreira	3,56	2,68	2,13	1,86	2,40
Gênero	**Masculino**	3,19	2,65	2,20	1,69	1,90
	Feminino	3,61	2,69	2,04	1,65	2,18

Fonte: O Autor

Tabela 6 - Médias das respostas da dimensão Coleta de Dados

	Domínio	**Coleta de Dados**				
	Questão	**Q13**	**Q14**	**Q19**	**Q20**	**Q21**
	Médias	1,76	1,55	4,29	3,60	2,18
Círculo Hierárquico	**Of Superiores**	1,72	1,29	4,25	3,35	2,13
	Of Interm.	1,69	1,06	4,00	3,19	2,00
	Of Subalernos	1,83	1,77	4,43	4,02	2,26
	Graduados	1,68	1,54	4,20	3,48	2,08
	Praças	1,88	1,77	4,42	3,69	2,65
Vínculo	**Carreira**	1,71	1,44	4,20	3,43	2,09
	Temporário	1,84	1,76	4,48	3,99	2,39
Grupo Idade	**Sênior**	1,69	1,36	3,94	3,20	1,95
	Func. Ativa	1,75	1,57	4,36	3,72	2,18
	Jovem Adulto	1,89	1,78	4,57	3,81	2,76
Grupo Tempo de Serviço	**Sênior**	1,59	1,34	3,98	3,05	1,89
	Operacional	1,77	1,45	4,31	3,66	2,18
	Início Carreira	1,85	1,78	4,50	3,99	2,41
Gênero	**Masculino**	1,70	1,48	4,19	3,25	2,00
	Feminino	1,82	1,64	4,42	4,11	2,44

Fonte: O Autor