

UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS TECNOLÓGICAS
CURSO DE FORMAÇÃO DE OFICIAIS BOMBEIRO MILITAR

JOÃO VICTOR DOS SANTOS SILVA

CONTRAINTELIGÊNCIA NA SEGURANÇA DE PESSOAL:
Aspectos importantes na conscientização dos cadetes da ABMJM

São Luís
2023

JOÃO VICTOR DOS SANTOS SILVA

CONTRAINTELIGÊNCIA NA SEGURANÇA DE PESSOAL:
Aspectos importantes na conscientização dos cadetes da ABMJM

Monografia apresentada ao Curso de Formação de Oficiais Bombeiro Militar da Universidade Estadual do Maranhão - UEMA, para obtenção da graduação em Bacharel em Segurança Pública e do Trabalho.

Orientador: Prof. Esp. **Paulo** Rogério dos Santos Ribeiro – Major QOCBM

São Luís
2023

Silva, João Victor dos Santos.

Contraineligência na segurança de pessoal: aspectos importantes na conscientização dos cadetes da ABMJM / João Victor dos Santos Silva – São Luís, 2023.

79 f

Monografia (Graduação) – Curso de Formação de Oficiais Bombeiro Militar, Universidade Estadual do Maranhão, 2023.

Orientador: Prof. Esp. Paulo Rogério dos Santos Ribeiro.

1.Contraineligência. 2.Segurança de pessoal. 3.Proteção de informações sensíveis. 4.Academia de Bombeiros Militar Josué Montello. I.Título.

CDU: 355.405

JOÃO VICTOR DOS SANTOS SILVA

CONTRAINTELIGÊNCIA NA SEGURANÇA DE PESSOAL: Aspectos importantes na conscientização dos cadetes da ABMJM

Proposta tecnológica apresentada ao Curso de Formação de Oficiais Bombeiro Militar da Universidade Estadual do Maranhão - UEMA, para obtenção da graduação em Bacharel em Segurança Pública e do Trabalho.

Aprovado em: 22/06/2023

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br PAULO ROGERIO DOS SANTOS RIBEIRO
Data: 27/06/2023 11:23:04-0300
Verifique em <https://validar.iti.gov.br>

Maj. QOCBM **Paulo** Rogério dos Santos Ribeiro (orientador)
Especialista em Gestão Pública
Instituto Federal da Bahia



PEDEI PAULO Lustosa Nogueira
MAJOR QOPM
RGz 16.044-PMMA
Matricula: 00418918-00

Maj. QOPM **Pedro Paulo** Lustosa Nogueira
Especialista em Gestão de Segurança Pública
Universidade Federal do Maranhão

**ANDREA DA
CONCEICAO**

VIANA:81941145353

Assinado de forma digital
por ANDREA DA CONCEICAO
VIANA:81941145353

Dados: 2023.06.27 13:11:58
-03'00'

Maj. QOPM **Andrea** da Conceição Viana
Especialista em Gestão de Segurança Pública
Universidade Federal do Maranhão

“Nos desafios que se apresentam, descobrimos a chance de superar nossas próprias limitações, tecendo uma história singular de coragem, aprendizado e vitórias”

.

AGRADECIMENTOS

A Deus, demonstro minha gratidão, reconhecendo que sem sua graça e direção, nada disso seria possível.

Em segundo lugar àqueles que foram pilares fundamentais em minha trajetória, proporcionando apoio e amor incondicional. À minha amada família meu pai, minha mãe, meu irmão e minha irmã expresso minha gratidão profunda por estarem sempre ao meu lado, incansáveis em seu apoio e encorajamento.

Agradeço especialmente à memória de meu avô, cuja sabedoria e inspiração continuam a guiar meus passos. Seus valores e ensinamentos ressoam em minha jornada, fortalecendo meu espírito e me impulsionando a buscar o melhor de mim.

Foi graças a essa rede de afeto, compreensão e dedicação que cheguei até aqui. Cada membro de minha família desempenhou um papel essencial na minha formação, motivando-me a perseguir meus sonhos com determinação e perseverança.

Gostaria também de expressar minha profunda gratidão aos amigos próximos que caminharam comigo desde os dias do Instituto Federal do Maranhão e aos meus irmãos de caserna. A vocês, meus companheiros de jornada, que compartilharam as alegrias e desafios dessa trajetória, os mais sinceros agradecimentos.

Agradeço ao meu orientador, Major Paulo Rogério dos Santos Ribeiro. Ao solicitar sua assistência, ele prontamente aceitou me auxiliar neste grande desafio, cumprindo com maestria sua missão.

Por fim, agradeço todos que participaram direta ou indiretamente na minha formação.

RESUMO

Este projeto tem como objetivo geral analisar a importância da contra-inteligência na segurança de pessoal visando a proteção de informações sensíveis pelos cadetes da Academia de Bombeiros Militar Josué Montello (ABMJM) e propor a conscientização em contra-inteligência para esses profissionais. Os objetivos específicos incluem identificar as ameaças mais comuns à segurança dos cadetes e das informações sob sua responsabilidade, elaborar uma cartilha didática com orientações de segurança, realizar uma revisão bibliográfica sobre contra-inteligência, propor um fluxograma de acompanhamento dos cadetes da ABMJM. A justificativa para este projeto se baseia na importância da contra-inteligência na proteção de informações sensíveis e os recursos humanos em diversas organizações, incluindo as instituições militares. Os cadetes lidam com emergências e têm acesso a informações sigilosas relacionadas à segurança pública e defesa civil, tornando a proteção dessas informações e ativos especialmente importante. A falta de conhecimento sobre essas técnicas pode prejudicar a efetividade das ações de segurança e proteção de informações sensíveis. Ao propor a conscientização em contra-inteligência específico para os cadetes, este projeto visa capacitar esses profissionais a proteger informações sensíveis e os recursos humanos, além de contribuir para a segurança pública e defesa civil. Investir em programas de capacitação e aprimoramento dos profissionais que lidam com informações sensíveis é fundamental para prevenir, detectar e enfrentar as ameaças à segurança, garantindo maior segurança e proteção não só para as informações, mas também para as próprias vidas dos profissionais e da sociedade em geral.

Palavras-chave: Contra-inteligência; Segurança de Pessoal; Proteção de Informações Sensíveis; Academia de Bombeiros Militar Josué Montello.

ABSTRACT

The general objective of this project is to analyze the importance of counterintelligence in the security of personnel in order to protect sensitive information and personal assets of the cadets of the Josué Montello Military Fire Academy (ABMJM) and to propose counterintelligence awareness for these professionals. Specific objectives include identifying the most common threats to the security of military firefighters and the information under their responsibility, preparing a didactic booklet with security guidelines, conducting a literature review on counterintelligence, proposing a flowchart for monitoring ABMJM cadets. The rationale for this project is based on the importance of counterintelligence in protecting sensitive information and personal assets in various organizations, including military institutions. Military firefighters deal with emergencies and have access to sensitive information relating to public safety and civil defense, making protecting this information and assets especially important. However, these professionals often do not receive adequate training in counterintelligence, which can leave them vulnerable to external and internal threats. In addition, the lack of knowledge about these techniques can impair the effectiveness of security actions and the protection of sensitive information. By proposing specific counterintelligence awareness for military firefighters, this project aims to enable these professionals to protect sensitive information and personal assets, in addition to contributing to public safety and civil defense in a more efficient and effective way. Investing in training and improvement programs for professionals who deal with sensitive information and personal assets is essential to prevent, detect and face security threats, ensuring greater security and protection not only for information and assets, but also for the lives of employees, professionals and society in general.

Keywords: Counterintelligence; Personnel security; Protection of sensitive information; Cadets; Josué Montello Military Fire Academy.

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ABMJM	Academia de Bombeiros Militar Josué Montello
CBMMA	Corpo de Bombeiro Militar do Maranhão
CD	Conselho de Disciplina
CDN	Conselho de Defesa Nacional
CSN	Conselho de Segurança Nacional
DNAI	Doutrina Nacional de Inteligência
DNISP	Doutrina Nacional de Inteligência de Segurança Pública
ISP	Inteligência de Segurança Pública
PSO	Plano de Segurança Orgânica
PNPC	Programa Nacional de Proteção do Conhecimento Sensível
SEGOR	Segurança Orgânica
SENASP	Secretaria Nacional de Segurança Pública
SFICI	Serviço Federal de Informações e Contrainformações
SISBIN	Sistema Brasileiro de Inteligência
UEMA	Universidade Estadual do Maranhão

LISTA DE GRÁFICOS

Gráfico 1 - Perfil dos participantes da pesquisa quanto ao ano de curso	46
Gráfico 2 - Idade dos participantes	47
Gráfico 3 - Nível de conhecimento sobre o tema	48
Gráfico 4 - Percepção de importância do tema	50
Gráfico 5 - Resposta à pergunta “Conhece sobre normas e legislação sobre o tema de segurança de pessoal”	51
Gráfico 6 - A ABMJM promove algum programa de conscientização sobre segurança de pessoal	52
Gráfico 7 - Importância de programas de conscientização de segurança de pessoal	53
Gráfico 8 - Quantas vezes o senhor(a) soube de incidentes dentro ou fora da ABMJM que comprometeu a Segurança de Pessoal.....	54
Gráfico 9 - Resposta à pergunta. “A ABMJM realiza avaliações periódicas da efetividade do programa de segurança pessoal”	55
Gráfico 10 - Importância dos militares mais antigos na promoção da cultura de segurança de pessoal na ABMJM	56
Gráfico 11 - Nível de conhecimento acerca de boas práticas de segurança na internet, uso de redes sociais e salvaguarda de informações sensíveis	57

LISTA DE FIGURAS

Figura 1- Ciclo PDCA.....	39
Figura 2 - Abordagem de Segurança.....	41
Figura 3 - Ação coordenada por definições.....	42
Figura 4 - Estudo de Situação de Contraineligência “da ABMJM” de 25/05/2023	43
Figura 5 - Estudo de Situação, item C	44
Figura 6 - Fluxograma de aplicação do ciclo PDCA focado em segurança de pessoal e compartilhamento de informações	60

SUMÁRIO

1 INTRODUÇÃO	15
1.1 Objetivos	17
1.1.1 Objetivo geral.....	17
1.1.3 Objetivos específicos.....	17
1.2 Justificativa	17
2 REFERENCIAL TEÓRICO	18
2.1 A Atividade de Inteligência no Brasil	18
2.1.1 Base Legal da Atividade de Inteligência.....	18
2.2 Legislação de Inteligência para os Estados da Federação	21
2.3 Doutrina Nacional de Inteligência de Segurança Pública	23
2.4 Ramos da Atividade de Inteligência de Segurança Pública	24
2.5 Atividade do Bombeiro Militar	25
2.5.1 Ativos.....	25
2.5.2 Ameaças	26
2.6 Contrainteligência	27
2.6.1 Segurança orgânica (SEGOR)	29
2.7 Segurança da Informação e Recursos Humanos	30
2.7.1 Seleção de Pessoal	32
2.7.2 Informações sensíveis	33
2.7.3 Uso das redes sociais	34
2.7.4 Engenharia Social.....	35
2.7.5 Integridade física.....	36
2.7.6 Segurança de pessoal no mundo corporativo	36
2.8 Ferramentas de Gestão de Segurança Pessoal	38
2.8.1 Ciclo PDCA	38
2.8.2 Gestão de segurança organizacional	39
2.8.3 Plano de treinamento e conscientização	41
2.9 Aspectos Importantes na Segurança de Pessoal na ABMJM	43
3 METODOLOGIA	44
4 RESULTADOS E DISCUSSÃO	46
4.1. Caracterização dos Participantes.....	46
4.2. Nível de Conscientização dos Participantes em Relação à Segurança de Pessoal	47
4.3 Avaliação de Programa de Conscientização em Segurança de Pessoal Realizados pela ABMJM.....	52
4.4 Sugestão de Promoção de Curso de Extensão em Segurança de Pessoal na ABMJM.....	58
5 CONCLUSÃO	62
5.1. Considerações finais	62
5.2. Limitações do estudo	63
5.3. Contribuições para a área de segurança de pessoal	63
5.4. Recomendações para futuras pesquisas	63
REFERÊNCIAS	65
APÊNDICES	70
APÊNDICE A: QUESTIONÁRIO UTILIZADO NA PESQUISA	71
APÊNDICE B: CARTILHA DE CONTRAINTELIGÊNCIA PARA BOMBEIROS MILITARES	73

1 INTRODUÇÃO

O Corpo de Bombeiros Militar do Maranhão (CBMMA) desempenha uma ampla gama de atividades voltadas para a proteção e assistência da população. Na visão popular, os bombeiros são considerados especialistas no momento de maior necessidade, e seu trabalho é percebido como emocionante, cheio de desafios e aventuras.

Embora essas percepções sejam válidas, é importante ressaltar que há muitos desafios, limitações e riscos dessa profissão, um exemplo, são preocupações constantes por parte dos oficiais gestores, no tratamento da contrainteligência com foco na segurança de pessoal.

Nesse contexto, a Academia de Bombeiros Militar Josué Montello (ABMJM) desde 2006 em parceria com a Universidade Estadual do Maranhão (UEMA) promove a formação de cadetes a futuros oficiais do CBMMA. Cadetes estes que lidam no dia a dia com responsabilidades e desafios na manutenção da segurança institucional.

É importante que os órgãos públicos adotem medidas de segurança na seleção, contratação e acompanhamento dos servidores, bem como na gestão de informações e documentos confidenciais, o que não é diferente para os militares.

Além disso, a importância da conscientização dos cadetes sobre os aspectos da contrainteligência, por meio de treinamentos e campanhas de divulgação. Estes devem estar cientes dos riscos e das ameaças à segurança, bem como das medidas preventivas e dos procedimentos a serem adotadas, dessa forma, promovendo maior segurança para as atividades e o bom nome da instituição.

A Contrainteligência de Segurança de Pessoal é um tema crucial na área da segurança pública e privada. Segundo o Manual de Contrainteligência do Exército – EB70-MC-10.220 (BRASIL, 2019), segurança de recursos humanos tem a definição de grupo de medidas destinadas a preservar a integridade física e moral dos recursos humanos.

Ainda segundo o manual, a segurança de pessoal é uma atividade que envolve não apenas a identificação de ameaças externas, mas também a prevenção e detecção de possíveis agentes internos que possam comprometer a segurança da organização.

Segundo (BRASIL, 2019), a segurança de pessoal deve ser integrada com outras atividades de segurança, como a investigação de antecedentes, a análise de comportamento e o controle de acesso a informações sensíveis.

Conforme o Manual Técnico da Metodologia de Gestão de Riscos do Exército Brasileiro (EB20-MT-02.001), os indivíduos são considerados recursos humanos passíveis de cometer equívocos, tanto de maneira voluntária quanto involuntária.

O Manual de Contraineligência (BRASIL, 2019) também destaca a necessidade de se adotar medidas para proteger a infraestrutura crítica de sistemas e instalações necessários ao funcionamento de atividades essenciais da organização, cujo o principal ativo, é de recursos humano ou pessoal. É importante que esses sistemas sejam protegidos contra ameaças externas e internas, a fim de garantir a segurança e a estabilidade da organização

A gestão da segurança institucional é um elemento fundamental para o sucesso das atividades de conscientização do público alvo. Traçadas diretrizes e normas gerais é possível treinar e desenvolver o público alvo na identificação e neutralização de ameaças à segurança da organização.

É necessário a promoção uma cultura de segurança entre os colaboradores, conscientizando-os sobre a importância da proteção de informações sensíveis.

O treinamento de pessoal deve ser pautado na ética e na confiança mútua, uma vez que as atividades podem envolver o manuseio de informações confidenciais, para identificar e gerenciar possíveis riscos de vazamento de informações, garantindo a segurança da organização e de seus colaboradores.

Na contemporaneidade é factível a forte presença das redes sociais e a disseminação de informações em velocidades alarmantes, bem como uso de perfis falsos na busca de aplicação de golpes para vantagens próprias com uso de engenharia social por exemplo.

Assim, os cadetes da ABMJM também não estão livres de possíveis ataques como os mencionados e sendo representantes e fontes do CBMMA, são ativos selecionados para este estudo com ênfase na segurança de pessoal e boas prática com o propósito de avaliar seu conhecimento no assunto e promover capacitação adequada.

1.1 Objetivos

1.1.1 Objetivo geral

Analisar a importância da contrainteligência na proteção de informações sensíveis e do ativo pessoal, os cadetes, da ABMJM e propor a conscientização em contrainteligência para esses profissionais.

1.1.3 Objetivos específicos

- Elaborar uma cartilha didática com orientações de segurança para os cadetes da ABMJM, abordando medidas de proteção em redes sociais e outros cuidados.
- Realizar uma revisão bibliográfica sobre contrainteligência e suas aplicações na segurança de pessoal e informações.
- Avaliar a conscientização dos cadetes da ABMJM sobre a importância da contrainteligência na proteção de informações e ativos pessoais.

1.2 Justificativa

A contrainteligência é uma área fundamental para a proteção dos ativos, como exemplo, informações sensíveis, pessoal e outros, em diversas organizações, incluindo as instituições militares.

Na atividade bombeiro militar, a proteção desses ativos é especialmente importante, uma vez que eles lidam com emergências e têm acesso a informações sigilosas relacionadas à segurança pública e defesa civil.

No entanto, muitas vezes esses profissionais não recebem treinamento adequado em contrainteligência, o que pode deixá-los vulneráveis a ameaças externas e internas. A falta de conhecimento sobre esse ramo da inteligência, pode prejudicar a efetividade das ações de segurança e proteção de informações.

Portanto, é necessário analisar a importância da contrainteligência na proteção desses ativos, principalmente no que diz respeito as informações sensíveis e pessoal, os bombeiros militares, propondo a conscientização em contrainteligência para esses profissionais. O curso pode abordar tópicos como identificação de ameaças, segurança da informação, investigação e detecção de fraudes e manipulação.

Dessa forma, os bombeiros militares poderão estar mais preparados para proteger informações sensíveis e outros ativos, além de contribuir para a segurança pública e defesa civil de forma mais eficiente e efetiva.

Assim, é fundamental investir em programas de capacitação e aprimoramento dos profissionais que lidam com informações sensíveis e demais ativos, como os bombeiros militares, para que possam desenvolver habilidades e conhecimentos necessários para prevenir, detectar e enfrentar as ameaças à segurança das atividades desenvolvidas pelo Corpo de Bombeiros Militar do Maranhão.

2 REFERENCIAL TEÓRICO

Neste capítulo, serão apresentados os fundamentos teóricos que sustentam o presente estudo. O referencial teórico tem como objetivo fornecer embasamento conceitual e contextualizar o tema em análise, oferecendo uma visão panorâmica das principais teorias e pesquisas relevantes que contribuem para a compreensão do problema em questão. É por meio desse embasamento teórico que se busca identificar lacunas no conhecimento existente e justificar a relevância da pesquisa.

2.1 A Atividade de Inteligência no Brasil

Este tópico tem como objetivo analisar a evolução da atividade de inteligência no Brasil, fornecendo uma visão abrangente sobre sua origem, desenvolvimento e principais características. A atividade de inteligência desempenha um papel fundamental na segurança nacional e na formulação de políticas públicas, sendo responsável pela coleta, análise e produção de informações estratégicas para o Estado.

2.1.1 Base legal da Atividade de Inteligência

A atuação da inteligência no Brasil, conforme apontado por Cruz (2013), teve suas origens voltadas para atender às demandas da polícia política e fornecer assessoria aos governos, especialmente por meio do Conselho de Defesa Nacional, estabelecido em 1927. Nesse período, o objetivo principal era o controle dos opositores ao regime político vigente.

Ainda segundo o autor, a polícia política é uma forma de especialização das atividades policiais, que tem como objetivo a prevenção, o conhecimento, a classificação, o controle e a repressão de indivíduos, grupos, associações e movimentos que possam estar envolvidos em atividades não aceitas pelo regime político estabelecido.

O Conselho de Defesa Nacional tinha como missão reunir informações sobre diversos aspectos relacionados à defesa do país conforme apontado por Figueiredo (2005). Ainda segundo o autor esse órgão carregava desde o início uma característica problemática: um mandato excessivamente amplo que permitia ao governo utilizá-lo de maneira arbitrária contra qualquer indivíduo. Assim afirma Junior:

As origens da atividade de Inteligência de Estado no Brasil datam de 1927 com a criação do Conselho de Defesa Nacional (CDN) sendo seguido, em 1946, pelo Serviço Federal de Informações e Contrainformações (SFICI), ambos sob forte influência das Forças Armadas (Junior, 2020, p.05).

Assim, a atividade de inteligência tem suas raízes na necessidade de integrar informações entre órgãos ligados a setores estratégicos do país, como as Forças Armadas e o Conselho de Defesa Nacional. Isso ocorre devido à influência que esses órgãos exercem no processo de tomada de decisões e na gestão governamental.

Segundo Júnior (2020), a importância do serviço de inteligência foi mantida ao longo das gestões por meio do Serviço Nacional de Informações (SNI), estabelecido em 1964 para substituir o Serviço Federal de Informações e Contrainformações (SCIFI).

Importante considerar que durante esse período, o serviço de inteligência permaneceu como uma prioridade na administração nacional, até o ano de 1984, sendo desenvolvida uma cultura organizacional sólida nesse contexto.

Ainda segundo o autor, contudo, apesar dos avanços proporcionados pelo SNI, a agência foi desmantelada em 1990, o que enfraqueceu as atividades de inteligência em desenvolvimento até então. Somente em 1995, o serviço foi restabelecido quando o Presidente da República submeteu uma medida provisória à Assembleia Nacional, autorizando a criação da Agência Brasileira de Inteligência (ABIN).

A Agência Brasileira de Inteligência (ABIN) foi criada pela Lei nº 9.883, de 7 de dezembro de 1999, que também instituiu o Sistema Brasileiro de Inteligência (SISBIN).

De acordo com a própria legislação, compete ao SISBIN obter, analisar e divulgar as informações necessárias ao processo decisório do poder executivo, além de proteger essas informações do acesso não autorizado por pessoas físicas ou jurídicas.

Segundo Júnior (2020), com a criação do SISBIN e sua regulamentação nº 4.378 de 13 de setembro de 2002, tornou-se possível um maior grau de integração de informações entre os órgãos da unidade federativa. Isso permite uma troca de informações mais eficiente e abrangente entre essas entidades.

Novellino (2020) destaca que a atividade de Inteligência, ao longo da história dos Estados Nacionais, passou por diversos momentos, independentemente da orientação político-ideológica ou das formas de governo em que estava inserida.

O autor ressalta que o processo de construção do conhecimento, abrangendo a coleta, reunião, análise, processamento e difusão de informações, evoluiu ao longo do tempo, resultou no atual nível de profissionalismo alcançado pela atividade de Inteligência.

No Brasil, a atividade de Inteligência é regulamentada pela Lei nº 9.883, de 7 de dezembro de 1999, como destaca Novellino (2020). Representa o marco legal dessa atividade no país, estabelecendo os princípios, diretrizes e competências relacionados à Inteligência nacional.

A legislação desempenha um papel fundamental na estruturação e no controle da atividade no Brasil.

A Lei nº 9.883/99 instituiu o Sistema Brasileiro de Inteligência (SISBIN), bem como criou o órgão diretor que é a Agência Brasileira de Inteligência (ABIN). Além desse marco legal, como orientadores da atividade de Inteligência brasileira, há outros importantes documentos doutrinários, como a Política Nacional de Inteligência (PNI). (NOVELLINO, 2020, p. 120).

De acordo com o §2º do art. 1º da Lei nº 9.883 de 7 de dezembro de 1999, inteligência é assim definida:

entende-se inteligência como atividade que objetiva a obtenção, análise e disseminação de conhecimentos, dentro e fora do território nacional, sobre os fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado (BRASIL, 1999, art. 1º, §2º).

E conforme o PNI (Plano Nacional de Inteligência) instituído pelo decreto Nº 8.793, de 29 de junho de 2016, a contrainteligência é uma atividade que visa prevenir, detectar, obstruir e neutralizar a inteligência adversa, bem como as ações que representam ameaças à segurança. Desempenha um papel fundamental na proteção de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado.

A atividade de Inteligência desempenha um papel crucial como instrumento dos Estados modernos. Assim conforme Novellino (2020), quando utilizada adequadamente, com marcos regulatórios bem definidos, a Inteligência se torna um recurso valioso e indispensável para auxiliar na manutenção do bem comum, da paz e da harmonia na sociedade.

Portanto, a importância da atividade de Inteligência é inegável, desde que seja exercida dentro de parâmetros éticos e legais, visando ao benefício coletivo.

Assim, é possível verificar que a atividade de inteligência no Brasil está amparada por diversas normas e leis, que definem sua base legal e regulamentam sua atuação. Tais normas visam garantir a proteção dos interesses nacionais e a segurança da sociedade brasileira.

2.2 Legislação de Inteligência para os Estados da Federação

É importante ressaltar que, no âmbito da legislação, o dispositivo de regulação foi estabelecido pela Lei nº 8.361, de 29 de dezembro de 2005. Isso ocorreu cerca de 6 anos após a promulgação da Lei nº 9.883/99, que instituiu a ABIN como órgão central de inteligência no Brasil, e aproximadamente 3 anos após a publicação do Decreto que regulamentou o funcionamento do SISBIN.

A cronologia em destaque evidencia que houve um tempo considerável de deliberação até que o sistema legislativo estadual efetivamente normalizasse o serviço de inteligência, seguindo as disposições federais mais recentes.

De acordo com a mencionada lei, o sistema em questão foi estabelecido com o objetivo de captar e processar informações relevantes para a tomada de decisões do Poder Executivo estadual, além de garantir a confidencialidade dos dados de interesse do estado, nos seguintes termos:

Art. 2º - O Sistema Estadual de Inteligência é responsável pelo processo de obtenção, análise e disseminação de informações necessárias ao processo decisório do Poder Executivo, em especial no tocante à segurança da sociedade e do Estado, bem como pela salvaguarda de assuntos sigilosos de interesse estadual, sempre observando os fundamentos da defesa do Estado Democrático de Direito, da dignidade da pessoa humana e da garantia dos direitos iguais dos cidadãos, bem como os demais preceitos constitucionais vigentes (BRASIL, 2005, art.2º).

A legislação define ainda sendo seus órgãos integrantes:

Art. 4º - Constituem o Sistema Estadual de Inteligência:
I - a Casa Civil, por meio do Centro Integrado de Inteligência, como órgão central do Sistema;
II - a Secretaria de Estado de Segurança Pública, por meio do Centro de Inteligência de Segurança Pública;
III - a Polícia Militar e o **Corpo de Bombeiros Militares, por meio dos seus órgãos de Inteligência**;
IV - a Secretaria de Estado de Justiça e Cidadania, por meio da sua estrutura de inteligência. (BRASIL, 2005, art.4º).

Dessa forma, o legislador, ao tratar da questão estadual, estabeleceu por meio de lei que o Corpo de Bombeiros Militar é um dos responsáveis pela inteligência atuando de forma integrada ao órgão central, seguindo os princípios de oportunidade e segurança. Suas atribuições incluem, entre outras:

Art. 6º - Compete aos órgãos que compõem o Sistema Estadual de Inteligência, no âmbito de suas competências:
I - produzir conhecimento em atendimento as prescrições dos planos e programas de inteligência decorrentes da política do órgão central do Sistema Estadual de Inteligência;
II - planejar e executar ações relativas a obtenção e integração de dados e informações;
III - fornecer ao órgão central do Sistema, para fins de integração, informações e conhecimentos específicos relacionados com defesa das instituições e dos interesses do Estado;
IV - estabelecer os respectivos mecanismos e procedimentos particulares necessários às comunicações e ao intercâmbio de informações e conhecimento no âmbito do Sistema, observando medidas e procedimentos de segurança e sigilo, sob a coordenação do Centro Integrado de Inteligência.(BRASIL, 2005, art.6º).

É importante ressaltar que cada instituição de segurança pública possui suas características distintas, bem como áreas de atuação e competências específicas. No entanto, quando se trata de inteligência, todas essas instituições têm um objetivo em comum: a produção e proteção de conhecimentos essenciais para os processos

decisórios. Essa abordagem deve estar presente em vários componentes da organização.

2.3 Doutrina Nacional de Inteligência de Segurança Pública

Segundo Hamada e Moreira (2017) a Secretaria Nacional de Segurança Pública (Senasp) propôs a primeira versão da Doutrina Nacional de Inteligência de Segurança Pública (DNISP) em 2007. Ao longo do tempo, devido à evolução das questões de segurança pública e da própria Inteligência de Segurança Pública (ISP), a DNISP passou por várias revisões e alcançou sua 4ª edição, sendo oficialmente publicada no Diário Oficial da União (DOU).

A Doutrina Nacional de Inteligência de Segurança Pública (DNISP) é um documento que estabelece as diretrizes e os procedimentos para a produção e o compartilhamento de informações entre os órgãos de segurança pública no Brasil.

De acordo com a DNISP, a inteligência é definida como "o processo de obtenção, análise e disseminação de informações que permitam identificar ameaças, riscos e vulnerabilidades que possam comprometer a ordem pública e a segurança das pessoas" (BRASIL, 2014, p. 10).

A DNISP destaca a importância da cooperação e integração entre os órgãos de segurança pública para o sucesso da produção de inteligência. Conforme afirmado na doutrina, "a troca de informações é a base para a produção de inteligência" (BRASIL, 2014, p. 15).

A DNISP estabelece que a produção de inteligência deve ser pautada pela legalidade, imparcialidade, integridade e ética, garantindo a proteção dos direitos fundamentais dos cidadãos.

A doutrina também reconhece a importância da análise de dados para a produção de inteligência. Segundo a DNISP, "a análise é a atividade que permite transformar informações em conhecimento útil e aplicável" (BRASIL, 2014, p. 20).

Ao analisar a DNISP nota-se que é fundamental que os órgãos de segurança pública desenvolvam capacidades técnicas e tecnológicas para a análise de dados e utilizem métodos e técnicas adequadas para a interpretação das informações coletadas.

A DNISP destaca ainda que a necessidade de que a produção de inteligência esteja voltada para a prevenção e a mitigação de riscos e ameaças à segurança pública. Conforme afirmado na doutrina, "a produção de inteligência é uma atividade que visa a prevenção de ameaças e riscos, evitando que ocorram situações de violência ou que a ordem pública seja comprometida" (BRASIL, 2014, p. 25).

2.4 Ramos da Atividade de Inteligência de Segurança Pública

A DNISP apresenta a atividade de ISP (Inteligência de Segurança Pública) como uma atividade que se divide em dois ramos principais: a Inteligência e a Contrainteligência.

Segundo a DNISP, primeira tem como objetivo produzir conhecimentos de interesse da Segurança Pública, enquanto a segunda se destina a produzir conhecimentos para neutralizar as ações adversas e proteger a atividade e a instituição a que pertence.

Ainda segundo a doutrina, o ramo da Inteligência de Segurança Pública é definido como a prática contínua e organizada de medidas especializadas com o objetivo de identificar, avaliar e monitorar ameaças de qualquer tipo, sejam elas presentes ou potenciais, dentro do campo da segurança pública.

Conforme estabelecido na Doutrina Nacional de Inteligência de Segurança Pública, a Contrainteligência é o campo dedicado à geração de conhecimento com o propósito de preservar a atividade de Inteligência e a integridade da instituição a que está vinculada, por meio da proteção e neutralização de ações adversas de qualquer natureza (BRASIL, 2014).

Dessa forma, o escopo do presente estudo é o ramo da Contrainteligência. Conforme o Manual de Campanha EB70-MC-10.220 – Contrainteligência (BRASIL, 2019), esse ramo é uma ferramenta eficaz em todos os escalões, sendo que suas ações e atividades não são responsabilidade única e exclusiva dos militares que compõem o alto escalão de comando, mas de todos os militares.

Apesar de serem ramos distintos, a DNISP destaca que a Inteligência e a Contrainteligência são interdependentes e inter-relacionadas. Ou seja, não há uma fronteira clara entre os dois ramos.

A atividade de inteligência precisa considerar aspectos de proteção e segurança da informação, assim como a contrainteligência deve estar em sintonia com as informações produzidas pela atividade de inteligência para cumprir seu papel.

Cada um desses ramos possui características e desafios específicos, exigindo a aplicação de técnicas e métodos adequados para a produção de inteligência. Além disso, é fundamental que haja cooperação e integração entre os órgãos de segurança pública que atuam em cada uma dessas áreas, garantindo a troca de informações e a produção de inteligência de qualidade.

2.5 Atividade do Bombeiro Militar

O Bombeiro Militar desempenha um papel crucial na proteção da vida, do patrimônio e do meio ambiente. Este item tem como objetivo analisar a atividade do Bombeiro Militar no contexto da segurança e contrainteligência.

2.5.1 Ativos

A ABMJM assim como qualquer outra instituição possui ativos tangíveis e intangíveis próprios de sua composição e produção cotidiana que formam a imagem, respeito e valor desta para com a sociedade, segundo a norma NBR ISO/IEC 27001:2013, ativo é qualquer coisa que tenha valor para a organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

A atividade de bombeiro militar é essencial para a segurança da população, atuando em diversas áreas de atendimento de emergências e desastres. Vide a Constituição Estadual do Maranhão em seu art. 116:

Art. 116 – O Corpo de Bombeiros Militar, órgão central do sistema de defesa civil do Estado, será estruturado por lei especial e tem as seguintes atribuições:

I – estabelecer e executar a Política Estadual de Defesa Civil, articulada com o sistema nacional de defesa civil; (modificado pela Emenda à Constituição nº 025, de 23/11/99).

II – estabelecer e executar as medidas de prevenção e combate a incêndio. (MARANHÃO, 1989, art. 116).

O corpo de cadetes é treinado para agir rapidamente em situações de risco, salvando vidas e protegendo o patrimônio público e privado, sendo parte essencial para o futuro do Corpo de Bombeiros Militar do Maranhão.

Entre os ativos mais importantes para a atividade de bombeiro militar, podemos mencionar as equipes especializadas para diferentes demandas de emergências, como incêndios, resgates em altura, salvamento aquático, atendimento pré-hospitalar, entre outros.

As equipes especializadas possuem treinamentos específicos e equipamentos adequados para cada tipo de situação, protegendo assim esse importante ativo, que são as operações bombeiro militar.

Os veículos de emergência, como auto bomba tanque (ABT), ambulâncias e viaturas de auto resgate (AR), são essenciais para o deslocamento rápido das equipes de bombeiros para o local da emergência.

Os veículos são equipados com materiais e equipamentos de proteção individual (EPIs) fundamentais para a segurança do bombeiro, como capacete, luvas, botas, roupas de proteção contra o fogo, entre outros, essenciais para as operações de salvamento e atendimento pré-hospitalar.

Ademais, há técnicas e treinamentos desenvolvidas por um intenso treinamento e capacitação, no aprendizado de especificidades para cada tipo de emergência. Esses treinamentos incluem simulados e exercícios práticos, que preparam o bombeiro militar para agir com segurança e eficiência em situações de risco.

A comunicação eficiente entre as equipes e com outros órgãos de segurança pública para a coordenação das operações de emergência é outro ativo sensível. Há a utilização de rádios e outros equipamentos de comunicação para manter contato com as equipes de emergência e informar sobre o andamento das operações com linguagem própria e terminologia comum para aqueles que pertencem a instituição.

No centro de todos estes ativos encontra-se o elo humano, o corpo de cadetes, o ativo mais importante deste estudo e ao mesmo tempo, porta mais frágil para a entrada de ameaças corruptivas a obtenção de informações e a sua própria segurança, ao serem representantes da segurança pública, do Corpo de Bombeiros Militar do Maranhão.

2.5.2 Ameaças

Devido à natureza das emergências e função pública desempenhada pelo enfrentam muitas ameaças. Algumas das principais ameaças que os bombeiros

militares enfrentam são desde incêndios, acidentes de trânsito, desastres naturais, atentados terroristas, produtos perigosos, mas também uso inadequado de suas informações e imagem.

Além destas ameaças, o ativo humano está sujeito a ações de espionagem, vazamento de informações confidenciais, manipulação de informações, invasões de sistemas e apropriação indevida de recursos.

Conforme a Doutrina Nacional da Atividade de Inteligência (DNAI), existem duas categorias de ameaças: intencionais e não intencionais.

Quando são intencionais, elas são chamadas de antagonismos, enquanto no caso de serem não intencionais, são denominadas de óbices.

Segundo Brasil (2016), ameaças são representadas por condições ou elementos que afetam negativamente a realização de objetivos, bem como a segurança de informações e conhecimentos sensíveis.

Ainda segundo a doutrina, ameaças intencionais, conhecidas como antagonismos, envolvem ações hostis perpetradas por agentes de inteligência adversos, com o propósito de atacar os interesses da instituição.

Os óbices representam ameaças não intencionais decorrentes de ações humanas e fatores imprevistos, frequentemente causados por agentes internos na organização. Essas ameaças podem resultar em perdas e danos à instituição devido à falta de habilidade, imprudência ou negligência desses agentes.

É necessário estratégias de segurança que visem a prevenção e o combate a essas ameaças, por meio de atividades de identificação, análise e neutralização de riscos e vulnerabilidades, assim como de proteção de ativos e informações sensíveis.

2.6 Contrainteligência

Segundo Gonçalves (2019), a necessidade primordial da contrainteligência nas diversas esferas organizacionais que valorizam a confidencialidade de suas atividades e informações sigilosas é indiscutível nos dias atuais. A contrainteligência tem como objetivo central prevenir e inibir a atuação da inteligência adversa.

De maneira ampla, conforme Gonçalves (2019), é possível afirmar que praticamente todas as instituições de Segurança Pública do país reconhecem a importância do desenvolvimento estratégico, tático, administrativo e operacional em

uma visão de contrainteligência como elementos indispensáveis ao desenvolvimento da efetividade em matéria de proteção institucional.

De acordo com Silveira (2021), a contrainteligência engloba comportamentos, atitudes preventivas, proatividade e a consciente adoção de medidas efetivas que são constantemente e ininterruptamente desenvolvidas, com o objetivo de antecipar potenciais ações hostis.

Ainda conforme Silveira (2021), as atividades de contrainteligência são caracterizadas por sua natureza dinâmica e flexível, exigindo uma aplicação constante e uma retroalimentação contínua devido às incertezas decorrentes das ameaças em constante evolução.

Conforme o Manual de Campanha EB70-MC-10.220 – Contrainteligência, seus objetivos são assim elencados:

1.2.4 OBJETIVOS DA CONTRAINTELIGÊNCIA

1.2.4.1 São objetivos da Contrainteligência:

a) Impedir que ações hostis de qualquer natureza:

- 1) provoquem danos à integridade física de pessoal militar ou civil;
- 2) comprometam dados, informações, conhecimentos e sistemas a eles relacionados;
- 3) levem à perda de armamento e outros materiais de emprego militar;
- 4) inviabilizem a utilização de áreas, instalações e meios de transporte; e
- 5) atentem contra os valores, os deveres e a ética militar no Exército.

b) Impedir a realização de atividades de espionagem, sabotagem, ação psicológica hostil, terrorismo ou desinformação.

c) Induzir o centro de decisão hostil a posicionar-se de forma equivocada (BRASIL, 2019, p. 4-4).

As ações de Contrainteligência foram categorizadas nos seguintes segmentos: a Segurança orgânica, visando prevenir e neutralizar ações adversas de qualquer natureza, a Segurança ativa são medidas proativas destinadas a detectar, identificar, avaliar, analisar e neutralizar as ações adversas e Segurança de Assuntos Internos, visam assessorar as ações de correição das instituições de Segurança Pública, (Brasil, 2014).

O foco do estudo está na segurança orgânica na medida de proteção do ativo humano, sendo a segurança pessoal uma de suas vertentes.

2.6.1 Segurança orgânica (SEGOR)

Segundo a DNISP, a Segurança Orgânica (SEGOR) pode ser assim definida:

A SEGOR é o conjunto de normas, medidas e procedimentos de caráter eminentemente defensivo, destinado a garantir o funcionamento da instituição, de modo a prevenir e obstruir as ações adversas de qualquer natureza. (Brasil, 2014, p. 44).

Ainda segundo a própria doutrina, a segurança orgânica envolve um conjunto integrado e planejado de medidas destinadas à proteção dos ativos institucionais, incluindo aspectos como pessoal, documentação, instalações, material, operações de ISP, comunicações, telemática e informática.

Conforme a abordagem de Ribeiro (2019), o conceito de segurança orgânica (SEGOR) pode ser compreendido como um conjunto de ações com o propósito de proteger e preservar o funcionamento de uma instituição.

A ênfase recai na proteção dos ativos institucionais, englobando tanto aqueles de natureza tangível, ou seja, objetos concretos que podem ser visualizados e tocados, quanto os ativos intangíveis, que são abstratos e de difícil manipulação física.

Segundo Horta (2016), a gestão da Segurança Institucional no âmbito da Administração Pública requer a definição de diretrizes e normas gerais para a elaboração de planos de segurança orgânica adaptados às características e responsabilidades de cada órgão público.

Nesse contexto, a segurança institucional deve priorizar o engajamento de todos os membros da organização em ações preventivas. Quando pautada pela ética e pela justiça, essa abordagem reverbera positivamente em toda a instituição, conferindo imunidade a qualquer tipo de ameaça.

É evidente a importância de implementar ações sistemáticas para assegurar a proteção da administração pública. Nesse contexto, organizações como a ABMJM, é fundamental adotar diretrizes e planos de segurança orgânica que possam subsidiar medidas preventivas.

Conforme a análise realizada por Ribeiro (2019), os ativos considerados de maior relevância na área de segurança são identificados pela doutrina como sendo os principais. Essa classificação é atribuída devido à necessidade de agir em conformidade com as medidas estabelecidas pela segurança orgânica.

E conforme Brasil (2014), a segurança orgânica tem como seus grupos de atuação a segurança de pessoal, segurança da documentação, segurança das instalações, segurança do material, segurança das comunicações, segurança da tecnologia da informação e segurança das operações, assim definidos:

5.3.1.1 Segurança de Pessoal, destina-se aos recursos humanos, no sentido de assegurar comportamentos adequados à salvaguarda de dados e conhecimentos sigilosos. 5.3.1.2 Segurança da Documentação Direcionada para a proteção dos Documentos de Inteligência, no sentido de evitar o comprometimento e/ou o vazamento. A Segurança da Documentação é garantida através do exato cumprimento dos regulamentos, instruções ou normas que regem a produção, a classificação, a expedição, o recebimento, o registro, o manuseio, a guarda, o arquivamento e a destruição de documentos sigilosos. 5.3.1.3 Segurança das Instalações, voltada para os locais onde são elaborados, tratados, manuseados ou guardados dados e conhecimentos sigilosos, além de materiais sensíveis, com a finalidade de salvaguardá-los. A Segurança das Instalações é obtida pela adoção de medidas de proteção geral, fiscalização e controle do acesso. 5.3.1.4 Segurança do Material, voltada à salvaguarda, preservação e controle do material, de modo a assegurar seu perfeito e contínuo funcionamento. 5.3.1.5 Segurança das Operações de ISP Voltada à proteção das ações operacionais realizadas pela AI. Essa proteção inclui, notadamente, os agentes, a instituição, a identificação do alvo e os objetivos da operação, 5.3.1.6 Segurança das Comunicações, voltada para os meios de comunicações, no sentido de salvaguardar dados e/ou conhecimentos, de modo a impedir ou a dificultar a interceptação, a transmissão do tráfego de dados e sinais. 5.3.1.7 Segurança da Tecnologia da Informação, destinada a preservar os sistemas de Tecnologia de Informação, de modo a garantir a continuidade do seu funcionamento, a integridade dos conhecimentos e o controle do acesso. (Brasil, 2014, p.44 -45).

Assim, o foco do nosso estudo está amparado na segurança de pessoal com a conscientização dos cadetes da ABMJM no que visem mantê-los em comportamentos aceitáveis que preservem a proteção de dados e conhecimentos de caráter sigiloso.

2.7 Segurança da Informação e Recursos Humanos

A segurança da informação é uma questão extremamente importante para as organizações, e o fator humano, ou seja, os colaboradores, é um dos elementos críticos nesse processo.

De acordo com Argollo (2017), as pessoas são o elo mais fraco na segurança da informação, pois podem ser responsáveis por incidentes de segurança, de forma intencional ou não intencional. Nesse sentido, a conscientização e a capacitação dos colaboradores são fundamentais para garantir a segurança da informação.

Segundo Barbosa e Silva (2016), a educação em segurança da informação deve ser vista como um processo contínuo, que envolve não apenas treinamento técnico, mas também a conscientização sobre a importância da segurança da informação e o papel de cada indivíduo na proteção dos dados da organização.

Conforme o Manual de Campanha EB70-MC-10.220 – Contraineligência, a segurança dos recursos humanos compreende um conjunto de medidas que visam garantir a proteção física e moral dos profissionais do Exército Brasileiro.

A avaliação de riscos e vulnerabilidades relacionados à Segurança dos Recursos Humanos deve ser realizada considerando a atuação de agentes antagônicos de qualquer natureza contra a organização.

Para o sucesso das ações de segurança nessa área, é fundamental a conscientização do público interno sobre as possíveis ameaças, além da implementação de treinamentos e soluções de qualidade (BRASIL, 2019).

Contexto da segurança dos recursos humanos, é importante considerar a duração do tempo em que um indivíduo permanece desempenhando atividades sensíveis por um período prolongado. Isso pode representar riscos, como o compartilhamento de informações sigilosas e o conhecimento de dados pessoais sobre os membros da instituição.

Dessa forma, o Manual de Campanha EB70-MC-10.220 - Contraineligência ressalta que, com o objetivo de minimizar esse tipo de problema, é fundamental que ocorra a rotatividade de funções sempre que necessário, inclusive para os agentes que atuam na área de contraineligência (BRASIL, 2019).

Cabe salientar que na segurança de pessoal é importante considerar três medidas que visam garantir a integridade da instituição militar: antes do ingresso do indivíduo, durante sua atividade e após seu desligamento. Para isso, é necessário realizar investigações sociais e verificar antecedentes criminais, a fim de avaliar o perfil dos candidatos e minimizar possíveis riscos para a organização.

As políticas de segurança da informação devem ser claras e objetivas, e devem ser comunicadas de forma efetiva para todos os colaboradores. Segundo Hintzbergen (2015), as políticas de segurança da informação devem abranger aspectos como o uso adequado de senhas, a proteção de dispositivos móveis, a proteção de informações confidenciais, entre outros.

2.7.1 Seleção de Pessoal

A seleção de pessoal também é um aspecto importantes a serem considerados na segurança da informação. Segundo Castells (2018), as organizações devem implementar processos de seleção rigorosos para garantir que os novos colaboradores sejam confiáveis e estejam comprometidos com a segurança da informação.

Da mesma forma, nos concursos públicos, especialmente na área de segurança pública, a avaliação teórica do conteúdo do edital é apenas a primeira etapa de um processo que inclui avaliação documental, avaliação psicotécnica, investigação social e teste físico, a fim de determinar o perfil básico adequado para a profissão.

Todos os anos por meio do Processo Seletivo de Acesso à Educação Superior da Universidade Estadual do Maranhão (PAES UEMA) em parceria com o Corpo de Bombeiros Militar do Maranhão são selecionados candidatos a fazer parte do Curso de Formação de Oficiais Bombeiro Militar e adentrar na Academia de Bombeiro Militar Josué Montello e uma das etapas mais importantes é a de investigação social dos candidatos com a verificação de seus antecedentes.

Da mesma forma, nos concursos públicos, especialmente na área de segurança pública, a avaliação teórica do conteúdo do edital é apenas a primeira etapa de um processo que inclui avaliação documental, avaliação psicotécnica, investigação social e teste físico, a fim de determinar o perfil básico adequado para a profissão.

É importante que as organizações realizem verificações de antecedentes e referências dos candidatos, a fim de minimizar os riscos de contratação de indivíduos com histórico de comportamento inadequado ou criminoso.

Branco, Schaufert e Lento (2014) destacam que a investigação de segurança deve incluir a pesquisa dos antecedentes do candidato, onde o entrevistador deve examinar o passado do candidato, as funções e empregos que ele já ocupou.

Além disso, é necessário acessar atestados e certidões que comprovem o caráter moral do candidato, como a ausência de processos, dívidas e problemas eleitorais, entre outros.

É importante ressaltar que muitas das informações relevantes para a investigação de segurança podem ser facilmente acessadas pelo entrevistador na rede pública da internet.

Através de sites oficiais do governo, é possível consultar dados como nome completo, data de nascimento, CPF ou RG para obter informações importantes sobre antecedentes criminais, processos judiciais e dívidas, dentre outros aspectos que possam comprometer a segurança do cargo a ser ocupado.

Por fim, é importante que as organizações criem uma cultura de segurança da informação, na qual todos os colaboradores estejam comprometidos com a proteção dos dados da organização.

Segundo Whitman e Mattord (2018), a cultura de segurança da informação deve ser promovida e incentivada em todos os níveis da organização, desde a alta direção até os colaboradores operacionais.

2.7.2 Informações sensíveis

As informações sensíveis são dados que, em caso de acesso não autorizado, podem causar danos significativos às pessoas, organizações ou governos. De acordo com Gonçalves (2019), as informações sensíveis podem incluir informações pessoais, financeiras, estratégicas, entre outras.

Para proteger as informações sensíveis, as organizações devem implementar medidas de segurança da informação adequadas. Segundo Ross et al. (2019), as medidas de segurança da informação devem incluir a classificação das informações sensíveis de acordo com seu nível de criticidade e a implementação de controles de acesso adequados.

Outro aspecto importante é o treinamento e conscientização dos colaboradores sobre a importância da segurança da informação e o tratamento adequado das informações sensíveis.

Segundo Kizza (2017), a conscientização dos colaboradores é fundamental para minimizar os riscos de vazamento de informações sensíveis e garantir a proteção dos dados da organização.

Por fim, é importante destacar que a proteção das informações sensíveis não se limita apenas às organizações, mas também é uma responsabilidade de cada indivíduo.

Segundo Whitman e Mattord (2018), as pessoas devem ser conscientizadas sobre a importância da privacidade e segurança da informação, e devem adotar práticas de segurança adequadas em suas atividades pessoais e profissionais.

2.7.3 Uso das redes sociais

Segundo Isoni (2009), conceito de redes tem suas raízes em várias disciplinas acadêmicas, como Antropologia e Sociologia, e os princípios essenciais da aplicação desses conceitos são definidos como interação, relacionamento, colaboração, compartilhamento, integração e complementaridade.

É por meio desses princípios que as redes sociais são estruturadas. De acordo com Marques (2007, p. 158), “a análise de redes sociais parte do pressuposto de que as relações sociais são a unidade básica da sociedade, em vez dos atributos individuais. Nesse sentido, o mundo social é ontologicamente formado por padrões de relação de diversos tipos e intensidades, em constante transformação”.

As redes sociais possibilitam a manutenção de contato com amigos, estabelecimento de novas conexões e a busca por indivíduos que compartilham interesses e ideias semelhantes.

Entretanto, muitas pessoas além de amigos e conhecidos estão interessados nas informações que as pessoas postam nas redes sociais, o cadete como armazenador de dados da organização e ao mesmo tempo seu representante, sendo responsável pela boa imagem da Corporação.

No entanto, o uso das redes sociais na contrainteligência também apresenta desafios. Segundo Karlova e Fischer (2013), as informações compartilhadas nas redes sociais podem ser facilmente manipuladas ou falsificadas, o que pode levar a análises equivocadas e tomadas de decisão inadequadas.

Assim é importante que a ABMJM estabeleça políticas claras para o uso das redes sociais, enquanto divulgação da intuição pelos cadetes, orientando-os sobre as práticas adequadas, bem como os riscos associados ao uso das redes sociais.

2.7.4 Engenharia Social

Segundo Watson, Mason e Ackroyd (2014), a engenharia social pode ser entendida como a aplicação de princípios da sociologia com o objetivo de solucionar problemas sociais específicos. Nessa abordagem, utiliza-se a arte de manipular intencionalmente o comportamento de alguém por meio de técnicas de comunicação especialmente construídas.

Além disso, conforme Mitnick e Simon (2002), a engenharia social envolve a habilidade de utilizar o comportamento humano como meio de quebrar a segurança, sem a necessidade de participar diretamente das ações. Por fim, a manipulação de informações sensíveis e a capacidade de influenciar indivíduos a executar determinadas ações são utilizadas para obter resultados relacionados

De acordo com Dolan (2004) a engenharia social é uma técnica que pode ser usada para persuadir ou enganar as pessoas a fim de obter informações confidenciais. Isso pode ser feito por meio de abordagens telefônicas, e-mails ou até mesmo pessoalmente.

No entanto, a engenharia social pode ser evitada por meio de treinamento e conscientização dos colaboradores. Conforme os autores, Watson, Mason e Ackroyd (2014), Mitnick e Simon (2002) e Dolan (2004), argumentam que, por meio do treinamento, os colaboradores podem ser capacitados a identificar e evitar táticas de engenharia social, ajudando a proteger as informações confidenciais da organização.

Além disso, é importante que as organizações adotem medidas de segurança para proteger as informações confidenciais e reduzir a vulnerabilidade à engenharia social.

De acordo com Programa Nacional de Proteção do Conhecimento Sensível (PNPC) (2021), as medidas de segurança incluem desconfiar e não realizar ações sem exigir comprovação, como clicar em anexos e links suspeitos, verificar a identidade das pessoas através de métodos como retornar ligações para conhecidos.

É fundamental evitar abrir anexos e acessar links desnecessários, conscientizando-se de que todos podem conter ameaças e limitar a quantidade de informações pessoais disponíveis repassadas para desconhecidos.

Em suma, a engenharia social pode ser uma ameaça à segurança das organizações, mas pode ser evitada por meio de treinamento e conscientização dos colaboradores, além de medidas de segurança adequadas.

2.7.5 Integridade física

A integridade física é um elemento crucial para a segurança de uma organização. No entanto, essa integridade pode ser comprometida por meio de ações que visam obter informações sigilosas por meio de manipulação ou engano, seja por meio da infiltração de agentes, sabotagem ou outras técnicas. Essas ameaças podem causar danos significativos, tanto físicos como financeiros, para a organização.

Para evitar essas ameaças, é fundamental adotar medidas de segurança adequadas. De acordo com Venâncio e Fernandes (2018), medidas como controle de acesso, monitoramento de instalações, treinamento dos funcionários e uso de tecnologia de segurança podem ajudar a proteger a integridade física da organização.

Portanto, a segurança física também pode ser comprometida por meio da própria equipe de segurança. Segundo Soares (2014), a manipulação ou suborno dos profissionais de segurança pode ser uma técnica eficaz para obter acesso a áreas restritas ou informações sigilosas.

Assim, é importante que as organizações adotem medidas de segurança não apenas para proteger sua integridade física, mas também para garantir a confiabilidade de seus próprios profissionais de segurança.

2.7.6 Segurança de pessoal no mundo corporativo

A segurança de pessoal é uma preocupação constante no mundo corporativo, pois as ameaças à integridade física e emocional dos funcionários podem afetar negativamente a produtividade e a imagem da empresa.

“Os ataques sempre objetivam furtar dados e informações sensíveis, as quais podem ser comercializadas ou empregadas para diversas práticas de chantagem, extorsão e ganhos financeiros” (OAB, 2015, p. 29). Essas ameaças podem afetar a segurança e privacidade dos funcionários, além de prejudicar a imagem da empresa.

Ainda segundo o mesmo autor, é fundamental compreender os padrões utilizados por funcionários, proprietários, gerentes, executivos e pelo público em geral

para cometer fraudes, além dos diversos fatores que motivam essas ações fraudulentas.

Para fortalecer a segurança e prevenir desvios e perdas financeiras nas organizações, é necessário direcionar os esforços para o elo mais vulnerável, ou seja, o ser humano. É essencial capacitá-lo, conscientizá-lo, responsabilizá-lo e destacar os benefícios de contribuir para o combate à corrupção e fraudes, visando a melhoria da sociedade como um todo.

Conforme o IIA (2017), o conceito de risco é definido como a possibilidade de ocorrência de um evento que pode impactar a realização dos objetivos, sendo avaliado considerando seu impacto e probabilidade. No contexto da segurança, o risco é compreendido como o potencial de uma ameaça específica explorar as vulnerabilidades de um ativo ou conjunto de ativos, resultando em prejuízo para a organização.

Conforme discutido por Talbot e Jakeman (2009), a segurança envolve estar protegido contra perigos e perdas. Essa proteção é alcançada através da mitigação das consequências adversas decorrentes de ações intencionais ou injustificadas de terceiros.

Importante observar que quando indivíduos ou ações violam essa condição de proteção, ocorre uma violação da segurança. Do ponto de vista técnico, a segurança significa que algo está protegido não apenas no momento presente, mas também ao longo do tempo, o que implica a implementação de medidas para garantir sua proteção contínua.

Nesse contexto, no mundo corporativo a segurança envolve a implementação de medidas para proteger ativos sensíveis que são essenciais para criar, capacitar e sustentar a capacidade organizacional. Esses ativos podem variar dependendo da natureza das atividades da organização, mas geralmente incluem informações confidenciais, ativos físicos valiosos, pessoas, processos exclusivos e capital intelectual.

De acordo com Spitzner (2014), é crucial que as empresas sejam capazes de otimizar seus recursos e tempo limitados, concentrando-se nos comportamentos que terão o maior impacto positivo.

Considerando que as pessoas representam uma grande vulnerabilidade nos sistemas de segurança, é importante promover a comunicação e fortalecer os comportamentos desejados, incentivando o comprometimento dos colaboradores.

Ainda segundo o autor, é essencial exigir que os colaboradores sigam as políticas e procedimentos estabelecidos, incluindo a oferta de treinamento em segurança e privacidade da informação. Isso garante que os colaboradores estejam cientes dos riscos e ameaças e estejam preparados para cumprir suas responsabilidades.

Além disso, é importante investir em programas de conscientização, promovendo uma avaliação contínua do desenvolvimento e impacto desses programas.

Assim as empresas devem adotar medidas de segurança não apenas para proteger a segurança de seus funcionários, mas também para garantir a confiabilidade de seus próprios profissionais.

2.8 Ferramentas de Gestão de Segurança Pessoal

Neste item, serão apresentadas as principais ferramentas de gestão de segurança pessoal utilizadas atualmente, visando proporcionar um ambiente seguro e protegido para indivíduos em diversos contextos.

2.8.1 Ciclo PDCA

De acordo com Oliveira (2019), o ciclo PDCA (Plan, Do, Check, Act) é uma ferramenta essencial para a gestão de pessoal na administração pública. Esse ciclo consiste em quatro etapas que devem ser aplicadas de forma contínua para garantir a efetividade das ações realizadas. O PDCA é um método de gerenciamento de processos que permite a realização de melhorias contínuas, por meio da identificação de problemas e da implementação de soluções.

A primeira etapa do ciclo PDCA é o planejamento (Plan), que consiste em estabelecer objetivos, metas e estratégias para a gestão de pessoal. A segunda etapa é a execução (Do), que envolve a implementação das ações planejadas. Em seguida, vem a etapa de verificação (Check), que tem como objetivo avaliar os resultados obtidos e compará-los com as metas estabelecidas.

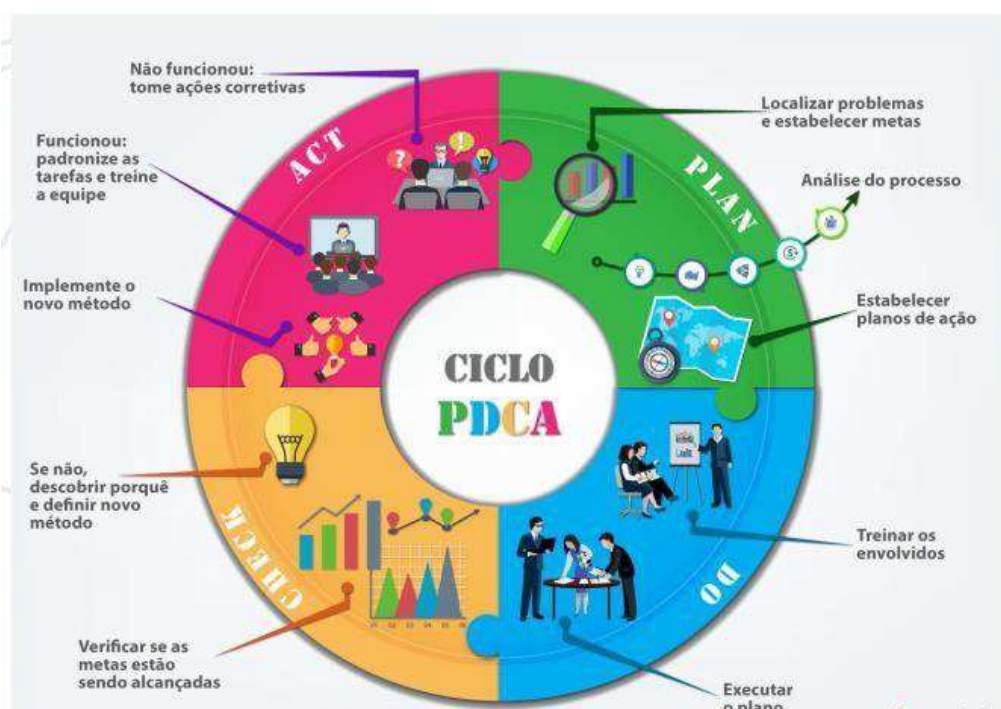
A etapa de ação (Act) consiste na análise dos resultados e na implementação de medidas corretivas para aprimorar o processo. Conforme Oliveira (2019), o ciclo

PDCA é uma metodologia simples e eficaz para a melhoria contínua dos processos e deve ser aplicado em todas as etapas da gestão de pessoal na administração pública.

Em conclusão, a aplicação do ciclo PDCA no contexto de conscientização dos cadetes da ABMJM oferece uma abordagem estruturada e sistemática para vulnerabilidades relacionadas a golpes financeiros, vazamento de informações sensíveis, engenharia social e uso inadequado de redes sociais.

Ao planejar, executar, verificar e agir de forma contínua, é possível desenvolver e aprimorar as medidas de proteção pessoal, fornecer orientações claras por meio de uma cartilha e capacitação dos cadetes, por exemplo, com conhecimentos e habilidades necessárias para enfrentar essas ameaças em constante evolução.

Figura 1- Ciclo PDCA



Fonte: Oliveira, 2019.

2.8.2 Gestão de segurança organizacional

Segundo Pacheco (2017), a construção de um Sistema de Gestão da Segurança Organizacional requer, primeiramente, uma análise e diagnóstico da situação atual em relação aos riscos e segurança.

Fundamental promover a conscientização de todos os funcionários responsáveis pela primeira linha de defesa da organização e por último, pela operacionalização de um plano para um Programa de Gestão de Segurança.

Ainda segundo o autor, A Política de Segurança tem como objetivo oferecer diretrizes e apoio para a gestão da segurança, de acordo com os requisitos da organização e as leis e regulamentos aplicáveis. Ela engloba um conjunto de políticas operacionais, normas, diretrizes e métricas que são dedicadas à proteção dos ativos da organização.

Segundo Wake (2011), é fundamental reconhecer a importância da identificação dos ativos. É necessário compreender quais elementos precisam ser protegidos antes de buscar aprimorar a segurança. Somente ao identificar com clareza o que é considerado relevante, é possível estabelecer as medidas necessárias para garantir sua segurança.

Conforme Razzetti (2017), a gestão da Segurança Organizacional pode ser equiparada à gestão de qualquer outra missão em um comando militar. Assim como em outras áreas, é necessário estabelecer políticas, objetivos e parâmetros de risco, implementá-los, realizar treinamentos, realizar medições, realizar benchmarking e, em seguida, conduzir auditorias de forma contínua.

De acordo com a Promon Business & Technology Review (2005), a verdadeira essência de uma estratégia de Segurança está centrada nas pessoas, nos ativos e nos processos, ou seja, nos elementos que impulsionam a produtividade da organização.

Assim medidas de Segurança que dependem exclusivamente de ferramentas de segurança ou que se concentram apenas no cumprimento de regulamentações podem revelar-se ineficazes.

Figura 2 - Abordagem de Segurança



Fonte: Promon Business & Technology Review, 2005

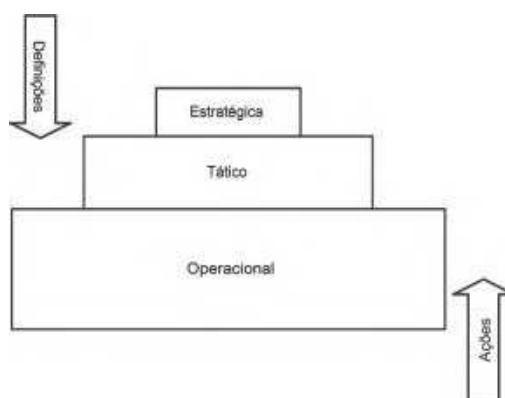
O cumprimento de regulamentos e normas não é sinônimo de segurança, não se está protegendo os ativos nem agregando valor à organização. Conforme Pacheco (2017), um dos desafios mais complexos enfrentados pelos profissionais de segurança é comunicar o valor da Segurança de forma efetiva.

Tendo em conta que ABMJM deve estabelecer, implementar, manter e melhorar de forma contínua a segurança de pessoal com os cadetes, a gestão da segurança organizacional faz uso do ciclo do PDCA buscando aperfeiçoamento e melhoria do Sistema, permitindo assegurar que os processos são dotados com recursos adequados e devidamente geridos e que as oportunidades são identificadas e estabelecidas.

2.8.3 Plano de treinamento e conscientização

Sendo a salvaguarda de assuntos sensíveis um problema institucional, envolvendo os aspectos humanos que sustentam a operação do Corpo de Bombeiros Militar do Maranhão, torna-se condição preponderante a mobilização dos escalões superiores.

Figura 3 - Ação coordenada por definições



Fonte: Sêmola, 2014

Segundo Sêmola (2014) a condição mencionada é essencial, uma vez que é impossível abordar de forma igualitária e simultânea as vulnerabilidades presentes em todos os ambientes e processos distribuídos, a menos que haja uma ação coordenada e, sobretudo, respaldada pela alta administração.

Segundo Horta (2016), a segurança institucional é de extrema importância nas organizações públicas, envolvendo atividades técnicas e especializadas que demandam profissionais altamente qualificados, sujeitos a treinamento contínuo e avaliação profissional regular.

Conforme Fonseca (2009), a principal meta de um programa de conscientização em segurança da informação em uma organização é influenciar os funcionários a alterar seus hábitos e motivá-los a participar do treinamento, com o propósito de conscientizá-los de sua importância fundamental na garantia da segurança.

Com a realização do estudo de situação da ABMJM, com o apoio dos cadetes do 3º ano, o mapeamento das vulnerabilidades destacadas em termos de conscientização do público, o apoio dos militares mais antigos nos acompanhamentos dos demais cadetes representa uma ação sugerida e possível de eficácia no combate desta vulnerabilidade, ação acompanhada de ferramentas como o ciclo PDCA.

2.9 Aspectos importantes na segurança de pessoal na ABMJM

A Academia de Bombeiros Militar Josué Montello (ABMJM) é composta por 3 turmas do Curso de Formação de Oficiais – CFO sendo formada por cadetes do 1º, 2º e 3º Ano, recebendo capacitações de comando, chefia e liderança sobre integrantes da tropa de bombeiros, nos serviços operacionais afetos à gerência de pessoal e de atividades-meio no âmbito administrativo e em ações tipicamente militares.

Conforme matriz curricular do curso em parceria com a UEMA, apenas no 3º Ano do CFO, os cadetes realizam a disciplina de inteligência e contrainteligência com carga horária de 60 horas. Fato esse que corroborou para busca do estudo da segurança de pessoal visto a falta de disciplina próprias do assunto ministradas para cadetes do 1º Ano e 2º Ano, e como já abordado, as pessoas são o elo mais importante e vulneráveis na segurança.

Visto o papel das instituições militares, é certo que a contrainteligência é um tema de extrema importância no Corpo de Bombeiros Militar do Maranhão (CBMMA) e conseqüentemente na ABMJM na proteção de seus ativos.

Atualmente, na ABMJM tal importância, pode ser constatado por meio da portaria que incumbiu o Major QOCBM Paulo Rogério dos Santos Ribeiro, subcomandante da ABMJM, as tratativas normativas, de levantamento e elaboração, do primeiro plano de segurança orgânica da academia com o auxílio dos cadetes do 3º Ano, 15ª turma do Curso de Formação de Oficiais Bombeiro Militar.

O plano contou com um estudo de situação que constatou desconhecimento das medidas de Segurança Orgânica indicando a necessidade de promover treinamentos e capacitações para conscientizar e educar os membros da unidade sobre as diretrizes e procedimentos de segurança.

Figura 4 - Estudo de Situação de Contrainteligência “da ABMJM” de 25/05/2023

(a) Alguns militares apresentam desconhecimento das medidas de Segurança Orgânica. Isso indica a necessidade de promover treinamentos e capacitações para conscientizar e educar os membros da unidade sobre as diretrizes e procedimentos de segurança. É fundamental garantir que todos os militares tenham conhecimento adequado e estejam comprometidos em seguir as medidas de segurança estabelecidas.

Bem como reconhece a falta de programas de conscientização em contrainteligência.

Figura 5 - Estudo de Situação, item C

(c) A ABMJM carece de um programa completo de educação e conscientização em contrainteligência. É essencial implementar um programa abrangente que inclua treinamentos regulares, palestras e materiais educativos para promover a conscientização sobre as ameaças de segurança, a importância da contra inteligência e as medidas de proteção adequadas. Dessa forma,

Fonte: Estudo de Situação de Contrainteligência da ABMJM, 2023

Assim pode se constatar que a ABMJM reconhece a necessidade de treinamento contínuo, para que os cadetes estejam sempre atualizados e capacitados para enfrentar as mais diversas situações. Bem como a realização de programas de conscientização sobre segurança orgânica e de pessoal.

O uso de cartilhas também pode ser uma ferramenta importante na promoção da segurança de pessoal na ABMJM. As cartilhas são materiais didáticos que podem auxiliar na disseminação de informações relevantes, tais como os procedimentos corretos no uso de redes sociais, salvaguarda de informações sensíveis, evitar golpes financeiros e ataques de engenharia social que coloquem o pessoal em situação de risco.

Dessa forma, a adoção dessas medidas pode contribuir significativamente para a promoção da segurança de pessoal na ABMJM, garantindo a proteção dos bombeiros militares e a eficácia das atividades desenvolvidas pela instituição.

3 METODOLOGIA

A pesquisa realizada neste estudo utilizou metodologias de revisão bibliográfica e análise documental, além de pesquisa de campo, com aplicação de questionário com os cadetes da ABMJM.

Segundo Marconi e Lakatos (2018), o método de abordagem é caracterizado por uma ampla abordagem dos fenômenos da natureza e da sociedade em um nível mais abstrato.

A pesquisa contou com a abordagem indutiva, “nesse método, parte-se da observação de fatos ou fenômenos, cujas causas se deseja conhecer.”(GIL, 2011 p.10), a indução é parte de um processo mental em que a partir de dados particulares e suficientemente contatados infere-se uma verdade geral ou universal, não contida nas partes examinadas.

Conforme autores como Severino (2007), Cervo, Bervian e Silva (2007) e Gil (2008), a pesquisa bibliográfica envolve dados passados, ou seja, registros realizados por estudos anteriores que servem como base para o pesquisador compreender determinado tema ou problema e conforme Cellard (2008), a Análise Documental favorece o processo de maturação ou de evolução do grupo a ser estudado.

Para a revisão bibliográfica e análise documental, com abordagem indutiva, foi utilizado as obras de diversos autores, tais como: Marconi e Lakatos (2018), Gil (2008, 2011), Cervo, Bervian e Silva (2007), Cellard (2008) e Severino (2007). Esses autores são referências na área de metodologia de pesquisa e oferecem importantes contribuições para a realização de uma revisão bibliográfica e análise documental de qualidade.

Quanto às normas e regulamentos relacionados à segurança pessoal em ambiente de treinamento, foi utilizado a Doutrina Nacional de Inteligência e Segurança Pública e o EB70-MC-10.2020-Manual de Campanha de Contrainteligência, que abordam questões relacionadas comportamentos adequados à salvaguarda de dados e conhecimentos sigilosos e legislação vigente sobre o assunto.

Para a análise das estratégias de conscientização, foram utilizadas obras de autores como Sêmola (2014), Razetti (2017), Promon Business & Technology Review (2005) e Horta (2016), que discutem métodos e técnicas de conscientização e treinamento.

Na pesquisa de campo, foram aplicados questionários, sem a utilização de citação direta de autores. Entretanto, foram adotadas as normas da ABNT para a elaboração das questões e para a análise dos resultados obtidos.

Sendo assim, a pesquisa realizada neste estudo foi embasada em uma ampla revisão bibliográfica e análise documental, com a utilização de obras de renomados autores da área. Além disso, foram seguidas as normas da ABNT para a elaboração da pesquisa de campo e para a análise dos resultados obtidos.

4 RESULTADOS E DISCUSSÃO

No presente capítulo, serão apresentados os resultados e discussões que fundamentam o presente estudo. Os dados obtidos por meio da coleta e análise dos dados fornecem insights valiosos sobre o tema em análise.

A análise dos resultados permitiu uma compreensão aprofundada das questões em estudo e possibilitou a identificação de padrões, tendências e relações entre as variáveis investigadas. Além disso, as discussões em torno dos resultados obtidos foram embasadas pelo referencial teórico, que ofereceu uma visão panorâmica das principais teorias e pesquisas relevantes relacionadas ao tema.

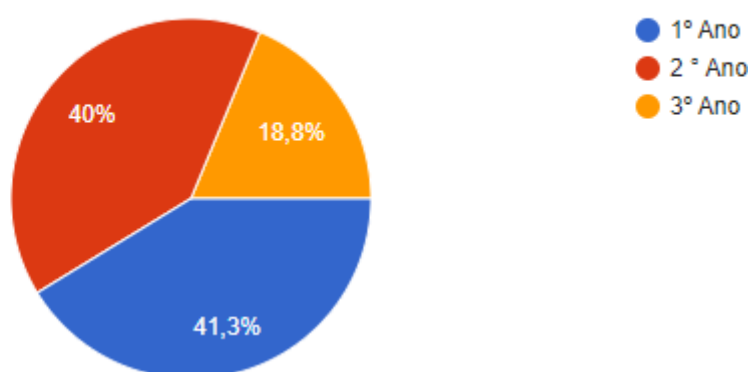
4.1. Caracterização dos participantes

O gráfico 01 apresenta a distribuição da quantidade de entrevistados divididos por grupos de cadetes na pesquisa realizada para este trabalho de conclusão de curso (TCC) na ABMJM.

Os cadetes incluídos são do: 1º Ano, 2º Ano e 3º Ano. Enquanto o gráfico 2 apresenta a distribuição destes cadetes por idade, com alta concentração de idade entre 22 a 28 anos.

Gráfico 1 - Perfil dos participantes da pesquisa quanto ao ano de curso

80 respostas



Fonte: Elaborado pelo autor (2023).

Gráfico 2 - Idade dos participantes



Fonte: Elaborado pelo autor (2023).

Observa-se que o maior número de entrevistados é a de cadetes do 1º e 2º ano totalizando 65 indivíduos. Isso indica que a amostra selecionada para a pesquisa possui uma representatividade significativa de cadetes das turmas iniciais de formação dentro da instituição estudada.

Essa ampla participação pode ser atribuída à disponibilidade e interesse dos cadetes em contribuir para a pesquisa, bem como à acessibilidade desses indivíduos em um ambiente acadêmico.

Em contrapartida, os cadetes do 3º ano apresentam uma quantidade de 15 representantes. Essa baixa participação pode ser explicada pela disponibilidade limitada desses militares para participar da pesquisa, devido a suas atribuições e responsabilidades no âmbito profissional.

4.2. Nível de conscientização dos participantes em relação à segurança de pessoal

O gráfico 03 apresenta a distribuição do nível de conscientização dos participantes em relação à segurança de pessoal, categorizando-os como muito baixo, baixo, razoável, bom e muito bom. A análise desses dados permite uma compreensão do grau de conhecimento e conscientização dos entrevistados sobre esse tema.

Gráfico 3 - Nível de conhecimento sobre o tema



Fonte: Elaborado pelo autor (2023).

Observa-se que a categoria com a maior quantidade de participantes é a de conscientização regular, totalizando 37 indivíduos. Isso sugere que a maioria dos entrevistados possui um nível intermediário de conhecimento e conscientização sobre a segurança de pessoal.

Essa conscientização razoável pode indicar que os participantes possuem um entendimento básico dos princípios e práticas relacionados à segurança de pessoal, mas ainda apresentam espaço para aprimoramento e aquisição de conhecimentos mais específicos.

Em seguida, temos participantes classificados como ruim ou péssimo e bom, cada categoria com 25 e 13 indivíduos, respectivamente. Essa diversidade nos níveis de conscientização sugere uma variação significativa nos conhecimentos e percepções dos entrevistados.

A presença de um grupo considerável com nível baixo de conscientização representado em sua maioria por cadetes do 1º e 2º ano indica a necessidade de intervenções educacionais e informativas para elevar o nível de conhecimento sobre segurança de pessoal deste público.

Por outro lado, a presença de participantes com nível muito bom de conscientização é encorajadora, indicando que uma parcela dos entrevistados possui um alto grau de conhecimento e está ciente das melhores práticas e medidas de segurança de pessoal, representados em sua maioria por cadetes do 3º Ano.

Os cadetes do 3º Ano podem servir como referência e promotores de conscientização em seus respectivos ambientes de trabalho, compartilhando suas experiências e conhecimentos com os cadetes do 1º e 2º ano.

Identificar um grupo com nível muito baixo de conscientização, representado por 25 indivíduos, é importante reconhecer a relevância de fornecer suporte e recursos adicionais para esses participantes a fim de elevar seu conhecimento e conscientização sobre segurança de pessoal.

A análise do gráfico 02 revela uma variedade nos níveis de conscientização dos participantes em relação à segurança de pessoal. Embora a conscientização regular seja a categoria mais frequente, há espaço para melhorias tanto nos níveis bons quanto nos muito baixos.

Ao identificar essas lacunas, torna-se possível desenvolver estratégias educacionais e informativas direcionadas, a fim de promover uma conscientização mais ampla e efetiva sobre a segurança de pessoal entre os participantes da pesquisa.

O gráfico 04 apresenta a distribuição do nível de conscientização dos participantes em relação à segurança de pessoal, categorizando-os como importante e muito importante. A análise desses dados permite compreender a percepção dos entrevistados em relação à relevância desse tema.

Observa-se que a maioria dos participantes, totalizando 62 indivíduos, classificou o nível de conscientização como "muito importante". Isso indica que esses entrevistados reconhecem a segurança de pessoal como um aspecto essencial e crucial em suas vidas e/ou ambiente de trabalho.

Essa alta valorização sugere que esses participantes estão cientes dos riscos e das ameaças à segurança pessoal e entendem a importância de adotar medidas preventivas e protetivas.

Temos um grupo menor, representado por 17 participantes, que classificou o nível de conscientização como "importante". Embora essa categoria tenha uma presença menos expressiva, ela ainda demonstra que esses indivíduos reconhecem a relevância da segurança de pessoal, embora possam ter uma percepção levemente menos intensa em comparação ao grupo "muito importante".

É importante considerar que esses participantes também têm consciência da importância de se preocupar com a segurança de si mesmos e de outras pessoas.

Gráfico 4 - Percepção de importância do tema



Fonte: Elaborado pelo autor (2023).

A predominância da percepção de que a segurança de pessoal é "muito importante" entre os entrevistados é um resultado positivo, pois indica uma conscientização elevada e uma atitude proativa em relação à segurança.

A consciência mais aguçada pode ser atribuída a diferentes fatores, como experiências pessoais, treinamento profissional e a própria conscientização dos riscos existentes.

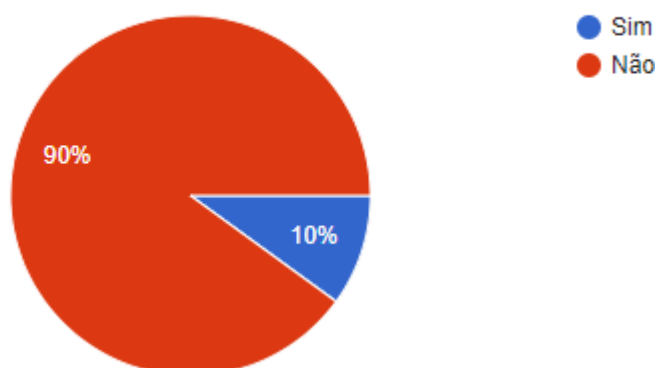
Essa análise sugere que os entrevistados estão motivados a adotar medidas de segurança, tanto em suas vidas pessoais quanto em seus contextos profissionais. É fundamental aproveitar essa conscientização e incentivar a implementação de práticas efetivas de segurança de pessoal, fornecendo orientações, treinamentos e recursos adequados para garantir a proteção e bem-estar dos indivíduos.

A análise do gráfico 04 revela que a maioria dos participantes possui um alto nível de conscientização em relação à segurança de pessoal, considerando-a como muito importante.

Já o gráfico 05 apresenta a distribuição do nível de conscientização dos participantes em relação à segurança de pessoal e seu conhecimento sobre normas e legislação relacionadas a esse tema. Os participantes foram categorizados como "Não" ou "Sim" em relação ao seu conhecimento sobre normas e legislação.

Gráfico 5 - Resposta à pergunta “Conhece sobre normas e legislação sobre o tema de segurança de pessoal”

80 respostas



Fonte: Elaborado pelo autor (2023).

A análise dos dados revela que a maioria esmagadora dos participantes, totalizando 72 indivíduos, indicou não possuir conhecimento sobre normas e legislação relacionadas à segurança de pessoal. Esse resultado demonstra uma lacuna significativa de informação e conhecimento entre os entrevistados nesse aspecto específico.

A falta de conhecimento sobre as normas e legislações pode ter diversas implicações, incluindo a possibilidade de não estarem familiarizados com as medidas de segurança adequadas e a dificuldade de tomar decisões informadas em situações relacionadas à segurança de pessoal.

Em contrapartida, apenas 8 participantes afirmaram ter conhecimento sobre normas e legislação relacionadas à segurança de pessoal. Essa quantidade reduzida sugere que uma parcela muito pequena dos entrevistados possui um conhecimento adequado sobre as regulamentações que regem a segurança de pessoal.

Essa análise enfatiza a importância de promover a conscientização e o conhecimento das normas e legislações relacionadas à segurança de pessoal entre os participantes. A falta de conhecimento nessa área pode comprometer a capacidade de tomar decisões seguras e implementar medidas adequadas de proteção pessoal.

O gráfico 05 indica uma deficiência acentuada de conhecimento sobre normas e legislação relacionadas à segurança de pessoal entre os participantes. A maioria

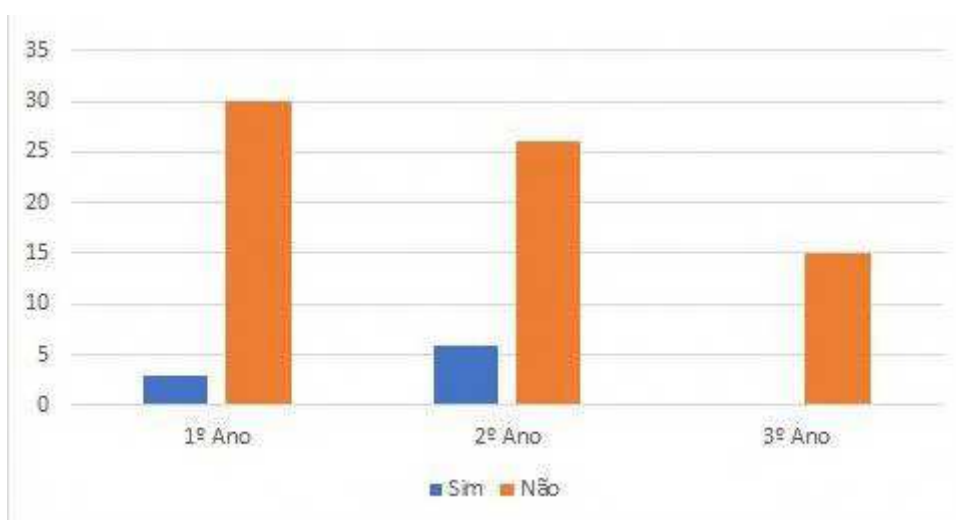
dos entrevistados afirmou não possuir esse conhecimento, destacando a necessidade de intervenções educacionais e informativas para preencher essa lacuna.

Promover a conscientização e o acesso a informações sobre as regulamentações existentes é fundamental para capacitar os participantes a adotarem medidas adequadas de segurança de pessoal e garantir um ambiente mais seguro para todos.

4.3 Avaliação de programa de conscientização em segurança de pessoal realizados pela ABMJM

O gráfico 06 apresenta a avaliação de programa de conscientização em segurança de pessoal oferecidos pela ABMJM em relação ao programa de conscientização sobre segurança de pessoal. Os participantes foram categorizados em dois grupos: Sim e Não.

Gráfico 6 - A ABMJM promove algum programa de conscientização sobre segurança de pessoal



Fonte: Elaborado pelo autor (2023).

A análise dos dados revela que uma parcela significativa dos entrevistados, totalizando 71 indivíduos, indicou que o programa de conscientização sobre segurança de pessoal não é realizado pela ABMJM.

Esse resultado aponta para uma lacuna na oferta de cursos de extensão voltados para a conscientização sobre segurança de pessoal na instituição.

A ausência desse programa pode limitar a capacidade dos participantes de adquirir conhecimentos e habilidades relacionadas à segurança pessoal, o que pode impactar negativamente sua capacidade de tomar decisões informadas em relação à segurança.

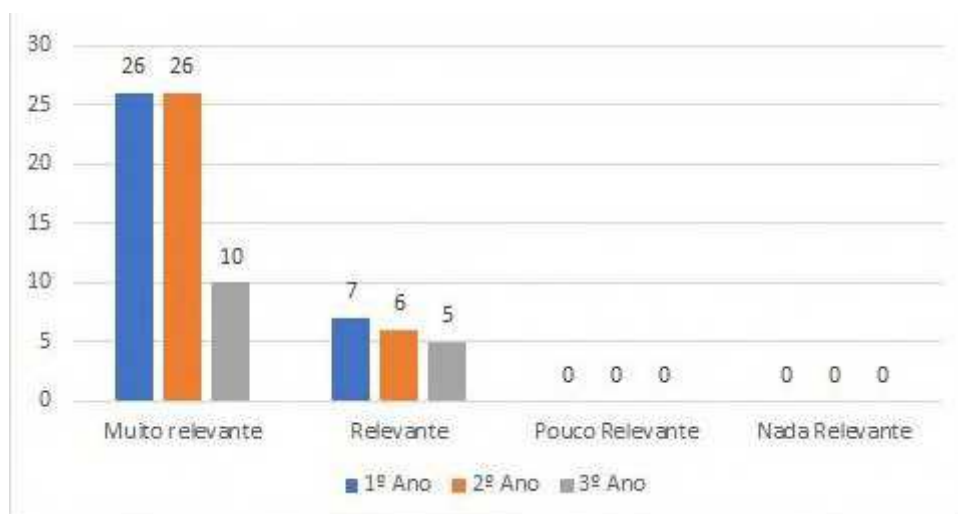
Por fim, 9 participantes afirmaram que o programa de conscientização é realizado. Esses indivíduos percebem que cursos de extensão e treinamento em segurança de pessoal podem promover a conscientização e fornecer conhecimentos relevantes nessa área.

Essa avaliação positiva demonstra que o programa pode atender às necessidades desses participantes, oferecendo-lhes as habilidades e informações necessárias para lidar com questões relacionadas à segurança de pessoal.

O gráfico 07 apresenta a avaliação em relação à importância dos programas de conscientização sobre segurança de pessoal. Os participantes foram categorizados em dois grupos: "Relevante", "Muito relevante", "Pouco Relevante" e "Nada relevante".

A análise dos dados revela que a maioria dos entrevistados, totalizando 62 indivíduos, avaliou os programas de conscientização de segurança de pessoal como "muito relevante". Esse resultado indica que os participantes percebem a importância fundamental desses programas na promoção de conhecimentos, habilidades e atitudes relacionadas à segurança pessoal.

Gráfico 7 - Importância de programas de conscientização de segurança de pessoal



Fonte: Elaborado pelo autor (2023).

Um grupo menor de entrevistados, representado por 18 participantes, avaliou os programas de conscientização como "relevante". Embora essa quantidade seja menor em comparação ao grupo anterior, ainda indica um reconhecimento significativo da importância desses programas.

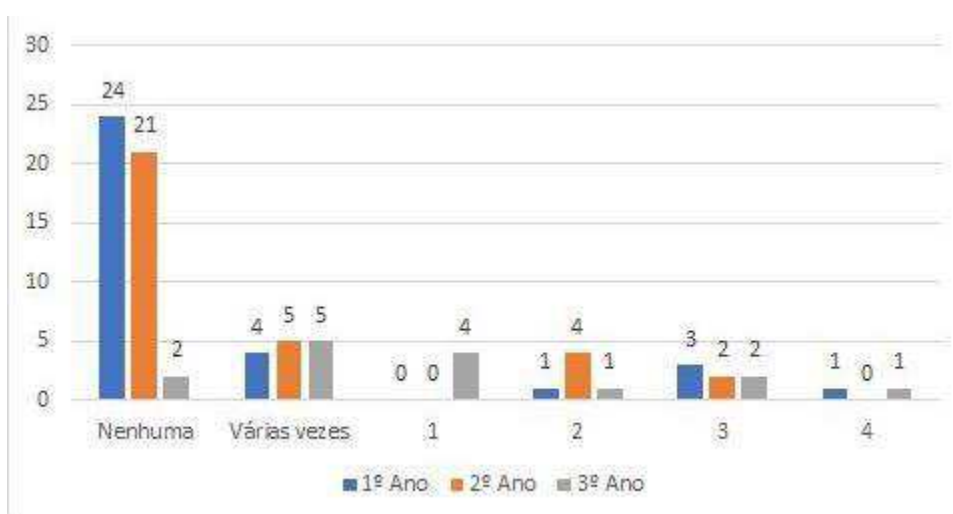
Esses participantes podem perceber a relevância de cursos de extensão em segurança de pessoal na criação de uma cultura de prevenção e proteção, bem como na capacitação dos indivíduos para tomar medidas adequadas de segurança em diferentes situações.

Enquanto o grupo "Pouco relevante" e "Nada relevante" não apresentaram respostas. O que representa significativo reconhecimento dos participantes em relação aos programas.

O gráfico 8 demonstrou o quantitativo de experiências dos cadetes com ocorrências que envolveram a segurança de pessoal, sendo que 14 afirmaram ter conhecimento de incidentes que comprometeram a segurança pessoal dentro ou fora da instituição em várias ocasiões.

Esses resultados sugerem que há uma falta de atenção ou cuidado por parte de alguns cadetes em relação a práticas de segurança, como o repasse de informações sigilosas a pessoas não autorizadas, uso inadequado de redes sociais e potenciais impactos negativos para a reputação da ABMJM e CBMMA.

Gráfico 8 - Quantas vezes o senhor(a) soube de incidentes dentro ou fora da ABMJM que comprometeu a Segurança de Pessoal



Fonte: Elaborado pelo autor (2023).

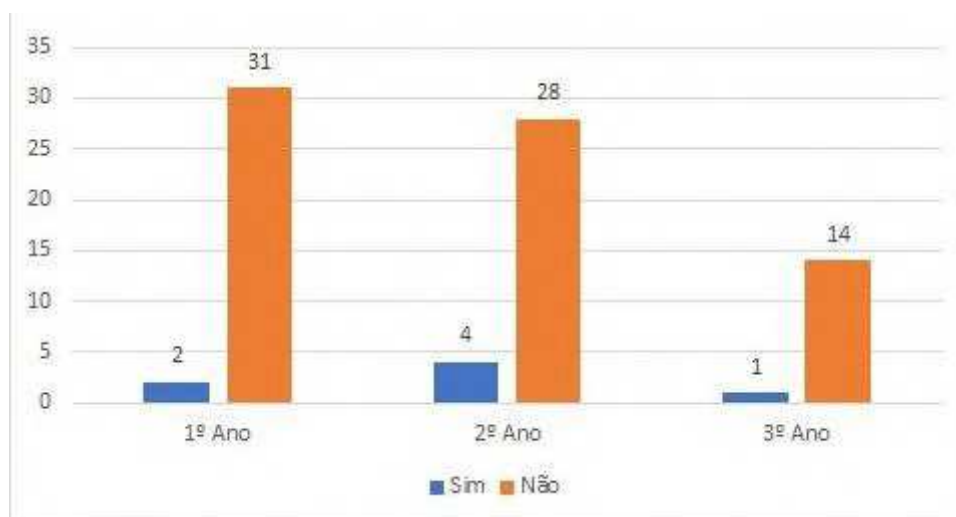
Além disso, 4 cadetes relataram ter conhecimento de incidentes ocorridos em uma única ocasião, enquanto 6 cadetes mencionaram ter ocorrido em duas ocasiões, e 7 cadetes afirmaram ter ocorrido em três ocasiões diferentes.

Essas respostas indicam que a ocorrência de incidentes comprometedores da segurança de pessoal não é um evento isolado, mas sim algo recorrente, o que ressalta a importância de medidas preventivas e educativas para os cadetes.

Ainda 47 respostas de 80 respostas relataram que não presenciaram nenhuma ocorrência, quantitativo que pode representar uma comunicação inadequada ou de uma falta de divulgação dessas ocorrências, que alguns cadetes podem ter presenciado incidentes, mas optaram por não relatar ou que estes cadetes estão conscientes e agindo de forma apropriada para evitar ameaças.

O gráfico 09 apresenta a avaliação de programas em segurança de pessoal oferecidos pela ABMJM em relação à realização de avaliações periódicas da efetividade do programa de segurança pessoal. Os participantes foram categorizados em dois grupos: "Não" e "Sim".

Gráfico 9 - Resposta à pergunta. "A ABMJM realiza avaliações periódicas da efetividade do programa de segurança pessoal"



Fonte: Elaborado pelo autor (2023).

A análise dos dados revela que a maioria dos entrevistados, totalizando 73 indivíduos, indicou que a ABMJM não realiza avaliações periódicas da efetividade do programa de segurança pessoal.

Esse resultado sugere uma lacuna na abordagem de monitoramento e avaliação do programa, o que pode limitar a capacidade da instituição em identificar áreas de melhoria e garantir a eficácia dos treinamentos e instruções oferecidos.

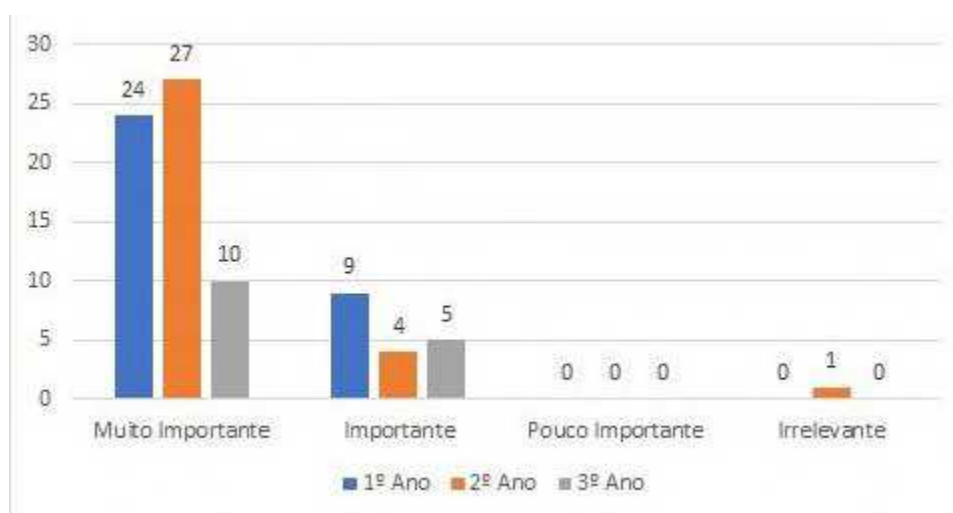
A falta de avaliações periódicas pode resultar em uma falta de feedback dos participantes, bem como na ausência de dados concretos para aprimorar o programa e adaptá-lo às necessidades em constante evolução dos alunos.

Por outro lado, um grupo menor de entrevistados, representado por 7 participantes, indicou que a ABMJM realiza avaliações periódicas da efetividade do programa de segurança pessoal. Esses participantes percebem a importância de avaliar regularmente o programa para identificar pontos fortes, lacunas e áreas que necessitam de melhorias.

A realização de avaliações periódicas permite que a instituição obtenha feedback dos participantes, avalie o impacto dos cursos e tome medidas corretivas para garantir a qualidade e a eficácia do programa de segurança pessoal.

O gráfico 10 indica que a maioria dos cadetes reconhece o papel dos militares mais antigos na promoção da cultura de segurança de pessoal na ABMJM como sendo muito importante. Isso demonstra a valorização e a importância atribuída à experiência e conhecimento dos militares mais experientes na instituição.

Gráfico 10 - Importância dos militares mais antigos na promoção da cultura de segurança de pessoal na ABMJM



Fonte: Elaborado pelo autor (2023).

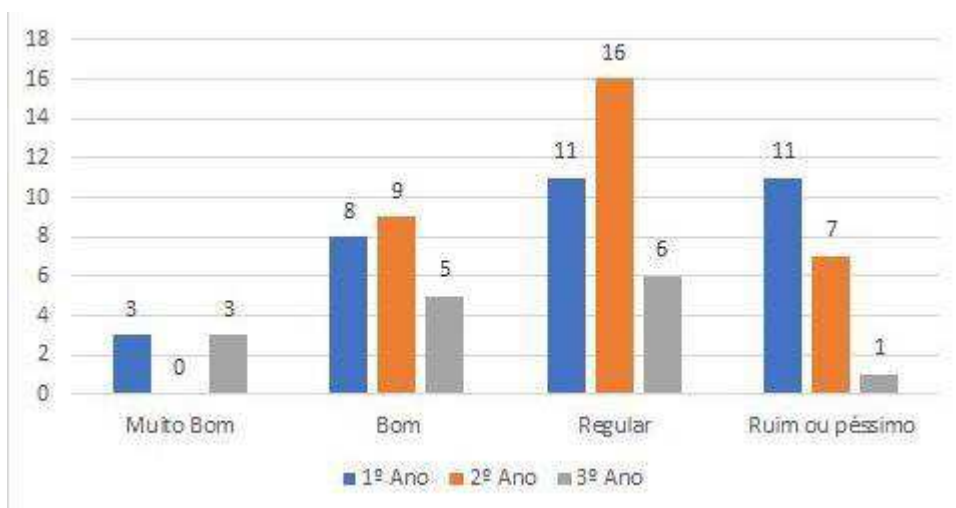
As 61 respostas indicando que é "muito importante" refletem a percepção de que os militares mais antigos desempenham um papel fundamental na disseminação e promoção das práticas de segurança de pessoal entre os cadetes.

Essa percepção sugere que os cadetes reconhecem a importância da transmissão de conhecimentos, orientações e melhores práticas pelos militares mais experientes, a fim de garantir a proteção e a segurança de todos os integrantes da instituição.

As 18 respostas indicando que é "importante" também demonstram a relevância atribuída aos militares mais antigos na promoção da cultura de segurança de pessoal. Embora possam não considerar seu papel como sendo de extrema importância, ainda reconhecem a contribuição significativa que esses militares podem oferecer na conscientização e no estabelecimento de comportamentos seguros entre os cadetes.

Analisando o gráfico 11, é possível observar que a maioria dos cadetes possui um nível de conhecimento considerado bom ou regular acerca de boas práticas de segurança na internet, uso de redes sociais e salvaguarda de informações sensíveis. Isso indica que existe uma base de conhecimento entre os cadetes, porém ainda há espaço para aprimoramentos.

Gráfico 11 - Nível de conhecimento acerca de boas práticas de segurança na internet, uso de redes sociais e salvaguarda de informações sensíveis



Fonte: Elaborado pelo autor (2023)

Dentre as respostas, 6 indicaram um nível de conhecimento considerado muito bom, demonstrando que alguns cadetes possuem um entendimento avançado e estão

familiarizados com as melhores práticas de segurança online e proteção de informações sensíveis.

No entanto, 33 respostas apontaram um nível de conhecimento regular, indicando que há uma parcela significativa de cadetes que reconhecem ter um conhecimento mediano sobre essas práticas. Isso destaca a necessidade de fornecer orientações e capacitação adicional para fortalecer a conscientização e o domínio dessas boas práticas de segurança.

Por fim, 19 respostas apontaram um nível de conhecimento ruim ou péssimo, revelando a existência de uma parcela dos cadetes que possui um conhecimento insuficiente ou limitado nessa área.

Os resultados reforçam a importância de desenvolver boas práticas de segurança para os cadetes, visando fornecer orientações claras e acessíveis que contribuam para a melhoria da conscientização e adoção de comportamentos seguros no uso da internet e das redes sociais.

Uma proposta para alcançar este objetivo é uso de uma cartilha (Apêndice B), devido a sua acessibilidade, pode ser facilmente distribuída e acessada por todos os cadetes, organização e síntese, uma cartilha é um recurso que permite organizar as informações de maneira clara e concisa, reforço da conscientização.

A cartilha pode servir como um lembrete constante das boas práticas de segurança, auxiliando na criação de uma cultura de segurança dentro da instituição e atualização contínua, a cartilha pode ser atualizada conforme novas ameaças e tendências em segurança digital surgem.

4.4 Sugestão de promoção de curso de extensão em segurança de pessoal na ABMJM

Em definição encontrada no Instituto Federal de São Paulo, corroborando com o Ministério da Educação, curso de extensão:

é a ação pedagógica de caráter teórico e prático, presencial ou a distância, planejada e organizada de modo sistemático para atender às necessidades da sociedade, visando ao desenvolvimento, à atualização e ao aperfeiçoamento de conhecimentos, com carga horária mínima de 20 horas e critérios de avaliação definidos. (IFSP,2020, p. 01).

Segundo LABFIN PROVAR (2019), um curso de extensão é considerado uma atividade complementar e opcional, que não faz parte do currículo da graduação. Essa modalidade permite ao profissional adquirir conhecimentos sobre temas que não foram abordados durante a graduação ou aprofundar-se em assuntos que foram tratados superficialmente durante esse período.

Os cursos de extensão, instrução e treinamento em segurança de pessoal no Corpo de Bombeiros Militar do Maranhão (CBMMA) desempenham um papel fundamental na capacitação e preparo dos militares para enfrentar desafios e riscos inerentes às suas atividades.

No entanto, observa-se que tal curso ainda não existe na ABMJM, o que há são orientações dadas pelos oficiais aos cadetes, durante as atividades do cotidiano do Curso de Formação de Oficiais, dessa forma carecem de um adequado planejamento estratégico e organização, para assim oferecer um amplo leque de qualificações para o efetivo.

A aplicabilidade da contrainteligência e a produção de conhecimento para neutralizar riscos potenciais são aspectos que merecem maior estímulo, a fim de quebrar paradigmas sobre o serviço de inteligência.

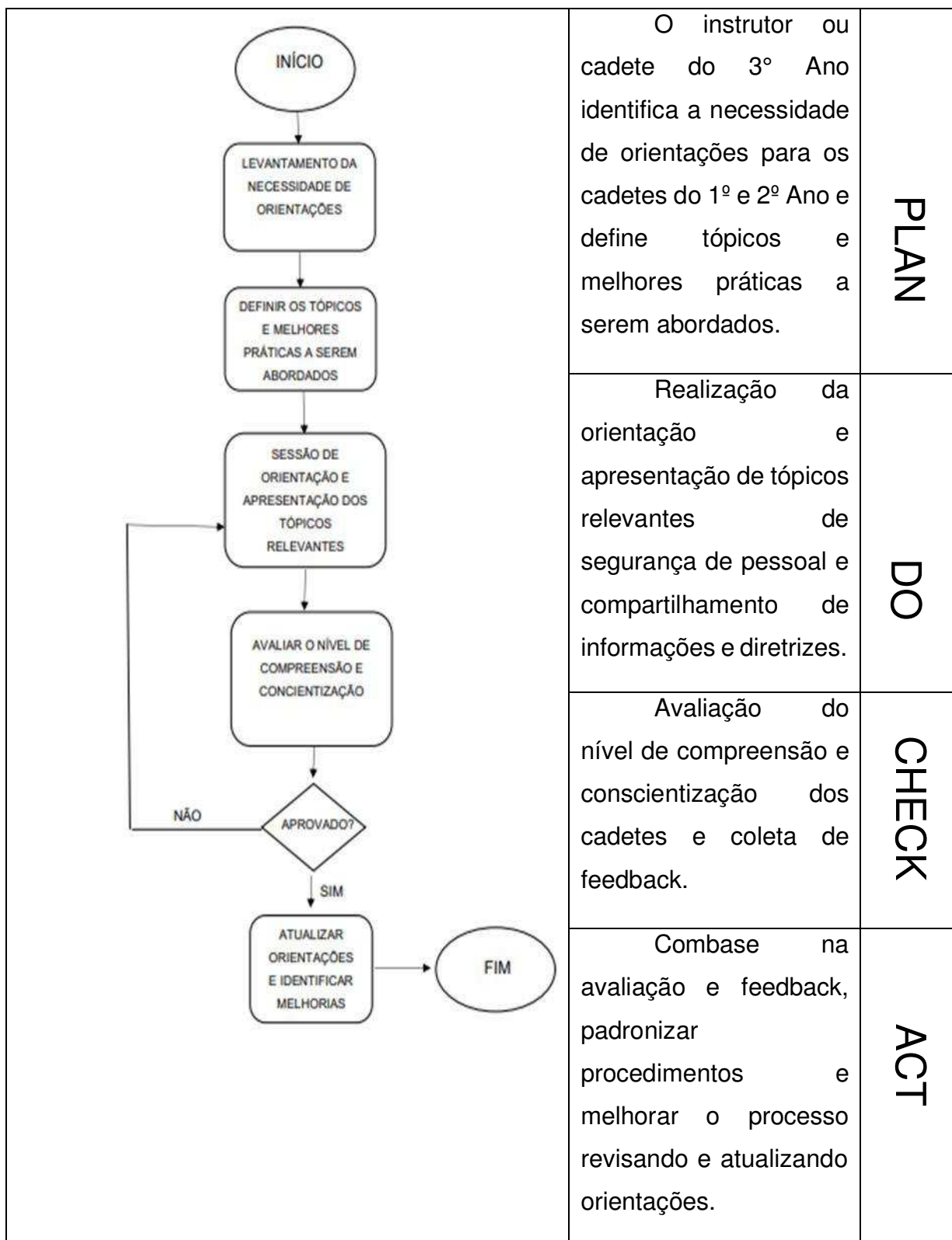
Uma das principais sugestões é a oferta dos cursos de extensão, instrução e treinamento em segurança de pessoal, de forma a alcançar um maior número de militares. Isso pode ser feito por meio de campanhas internas de conscientização, divulgação em meios de comunicação institucionais e parcerias com outras instituições de ensino e segurança.

Ademais é fundamental um planejamento estratégico e organização eficiente, estabelecendo critérios claros para a realização dos cursos, como objetivos, carga horária, requisitos e conteúdos programáticos bem estruturados.

Outra sugestão relevante é a capacitação contínua dos cadetes e a promoção da ampliação do conhecimento na ABMJM, pontos fundamentais da gestão da segurança institucional.

Para isso, é necessário o estabelecimento de programas de treinamento regulares, com a participação de instrutores especializados ou uso de cadetes do 3º ano com a abordagem de temas de engenharia social, uso das redes sociais, salvaguarda de informações sensíveis e relevantes para a segurança de pessoal. Com o uso do ciclo PDCA, uma sugestão de fluxo de acompanhamento contemplaria:

Figura 6 - Fluxograma de aplicação do ciclo PDCA focado em segurança de pessoal e compartilhamento de informações



Fonte: Elaborado pelo autor (2023).

A oferta de qualificações específicas, como cursos de especialização e pós-graduação, pode contribuir para o aprimoramento das habilidades e competências dos militares.

A aplicabilidade da contrainteligência e a produção de conhecimento também devem ser estimuladas. Essas práticas podem auxiliar na identificação e neutralização de riscos que a tropa pode ser acometida, proporcionando uma abordagem proativa em relação à segurança de pessoal.

Sendo fundamental fomentar a pesquisa e o desenvolvimento de técnicas e estratégias inovadoras, rompendo com paradigmas existentes no serviço de inteligência

Diante das sugestões apresentadas, fica evidente a importância de melhorar programas de conscientização em segurança de pessoal na ABMJM. A ampliação da divulgação, o planejamento estratégico e organização eficientes, a capacitação contínua dos militares.

A aplicabilidade da contrainteligência e a promoção de pesquisas sobre o assunto são medidas que podem aprimorar a formação e preparo do efetivo para enfrentar os desafios relacionados à segurança de pessoal.

Essas melhorias contribuirão para o fortalecimento institucional do Corpo de Bombeiros Militar do Maranhão e para a garantia da segurança dos militares em suas atividades diárias.

Para conscientizar e preparar todo o efetivo em relação a possíveis sinistros, é fundamental o estabelecimento de um programa de treinamento abrangente. Esse programa deve abordar diferentes cenários de risco e oferecer simulações práticas para que os militares possam desenvolver habilidades e tomar decisões assertivas em situações de emergência.

A realização de análises periódicas dos cursos e do desempenho dos militares pode fornecer *insights* valiosos para aprimorar o conteúdo e a eficácia do treinamento.

Outro aspecto relevante é o aumento do número de pesquisas sobre segurança de pessoal na ABMJM. A realização de estudos acadêmicos e técnicos nessa área pode fornecer subsídios para o aprimoramento dos cursos de extensão, bem como para o desenvolvimento de políticas e práticas mais eficientes no campo da segurança.

Destaca-se a importância de incentivar a participação dos militares em pesquisas, promovendo a troca de conhecimentos e o aprofundamento do tema.

Reforça-se a importância de uma gestão estratégica e organizada de cursos de extensão em segurança de pessoal, sendo necessário estabelecer metas claras, definir indicadores de desempenho e realizar avaliações periódicas para garantir sua efetividade.

Devido ao grau de especialidade, é fundamental contar com profissionais capacitados e com expertise na área de segurança, tanto como instrutores quanto como responsáveis pela coordenação dos cursos.

A implantação de cursos de extensão em segurança de pessoal na ABMJM requer um conjunto de ações que envolvem a ampliação da divulgação, o planejamento estratégico, a capacitação dos militares, a aplicabilidade da contrainteligência, a disponibilização de equipamentos de segurança individual, o incentivo à pesquisa e a gestão eficiente.

Ao implementar essas sugestões, espera-se elevar a qualidade e a eficácia dos cursos, promovendo uma preparação mais adequada dos militares e contribuindo para a segurança da instituição.

5 CONCLUSÃO

Com base na análise dos dados e das informações apresentadas, é possível concluir que os cursos de extensão, instrução e treinamento em segurança de pessoal oferecidos pela ABMJM são considerados relevantes e importantes pelos participantes.

A maioria dos entrevistados reconheceu a importância desses programas na conscientização e preparação para lidar com os desafios e riscos relacionados à segurança pessoal. No entanto, é necessário destacar algumas áreas de melhoria identificadas durante a análise.

5.1. Considerações finais

Os resultados indicaram que há uma necessidade de maior investimento na conscientização sobre normas e legislação relacionadas à segurança de pessoal. A maioria dos entrevistados revelou ter um conhecimento limitado nessa área, o que ressalta a importância de incorporar conteúdo específicos sobre normas e legislação nos cursos oferecidos pela ABMJM.

A realização de avaliações periódicas da efetividade do programa de segurança pessoal é essencial para garantir a qualidade e a eficácia dos cursos. Embora alguns participantes tenham indicado que o ABMJM realiza avaliações periódicas, a maioria relatou que essas avaliações são incipientes.

Recomenda-se que a ABMJM implemente um sistema de avaliação regular, com o objetivo de obter feedback dos participantes e identificar áreas de melhoria, como uso de cadetes do 3º Ano como auxiliares dos cadetes das demais turmas com uso do ciclo PDCA como forma de garantia da eficácia do treinamento na conscientização dos ativos.

5.2. Limitações do Estudo

É importante mencionar algumas limitações deste estudo. Em primeiro lugar, a análise foi baseada em uma amostra específica de entrevistados, o que pode limitar a generalização dos resultados para o contexto mais amplo do Corpo de Bombeiros Militar do Maranhão.

Além disso, a análise foi restrita aos dados fornecidos pelo questionário, sem considerar outros aspectos que poderiam influenciar a avaliação dos cursos de extensão em segurança de pessoal.

5.3. Contribuições para a área de segurança de pessoal

Este estudo contribui para a área de segurança de pessoal ao fornecer *insights* sobre a percepção dos participantes em relação aos cursos de extensão, instrução e treinamento oferecidos pela ABMJM.

Os resultados destacaram a importância da conscientização, do conhecimento sobre normas e legislação e da avaliação periódica do programa de segurança pessoal.

5.4. Recomendações para futuras pesquisas

Com base nas limitações identificadas e nas conclusões do estudo, recomenda-se que pesquisas futuras abordem aspectos adicionais relacionados aos cursos de extensão, treinamento e instrução em segurança de pessoal.

Algumas sugestões incluem: investigar a efetividade de diferentes abordagens pedagógicas utilizadas nos cursos, explorar a percepção dos participantes sobre a aplicabilidade prática dos conhecimentos adquiridos e analisar o impacto dos programas de conscientização na redução de incidentes de segurança pessoal.

Essas recomendações podem fornecer *insights* valiosos para aprimorar o programa de conscientização em segurança de pessoal, contribuindo para a formação de profissionais mais capacitados e conscientes dos desafios relacionados à segurança pessoal.

REFERÊNCIAS

ARGOLO, Anderson Lopes. **Segurança da informação: o ser humano como o elo mais fraco da corrente**. 2017. 44 pag. Monografia - Curso de Sistemas de Computação - Universidade Federal Fluminense, Niterói, 2017. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/12988/TCC_ANDERSON_LOPES_AR_GOLLO.pdf?sequence=4&isAllowed=y. Acesso em: 29 mai. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013. **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro. ABNT, 2013.

BARBOSA, Guilherme Augusto Ruani; SILVA, Maria Helena Barriviera. **Segurança da informação: a proteção contra o vazamento de dados e sua importância para as empresas privadas**. Disponível em: <https://pesquisafatec.com.br/ojs/index.php/efatec/article/view/105/101>. Acesso em: 6 jun. 2023.

BRANCO, André Haydt Castello; SCHAUFFERT, Fred Harry; LENTO, Luiz Otávio Botelho. **Inteligência e Segurança Pública**. Palhoça: UNISUL Virtual, 2014.

BRASIL. ABIN. **Programa Nacional de Proteção do Conhecimento Sensível: Boas Práticas**. Brasília, 2021. Disponível em: <https://www.gov.br/abin/pt-br/acesso-a-informacao/acoes-e-programas/PNPC/boas-praticas-1>. Acesso em: 11 jun. 2023.

BRASIL. **Decreto n. 8.793 29 de junho de 2016**. Fixa a Política Nacional de Inteligência – PNI. Disponível em: http://www.planalto.gov.br/ccivil/_03/_ato2015-2018/2016/decreto/D8793.htm.

BRASIL. **Decreto nº 4.376, de 13 de setembro de 2002**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência. 2002

BRASIL. **Lei nº 9.883 de 07 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN. Brasília, 2000.

BRASIL. Ministério da Defesa. Comando do Exército. Comando de Operações Terrestres. **EB70-MC-10.220 Manual de Campanha Contrainteligência**. Brasília, 2019.

BRASIL. **Portaria nº 59, de 26 de julho de 2018**. Instituir, no âmbito da Agência Brasileira de Inteligência - ABIN, o Programa Nacional de Proteção do Conhecimento Sensível - PNP. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/34380628/do1-2018-07-27-portaria-n-59-de-26-de-julho-de-2018-34380599 Acesso em: 14 de jun. de 2023. 2018/2016/decreto/D8793.html. Acesso em: 8 jun. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. ABIN. **Doutrina Nacional da Atividade de Inteligência: fundamentos doutrinários**. Brasília, 2016.

BRASIL. Presidência da República. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública – DNISP**. – 4. ed. rev. e atual. – Brasília: Secretaria Nacional de Segurança Pública, 2014.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 2018

CELLARD, A. A análise documental. In: POUPART, J. et al. **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Petrópolis, Vozes, 2008.

CERVO, A. L.; BERVIAN, P. A.; DA SILVA, R. **Metodologia científica**. 6 ed. São Paulo: Pearson Prentice Hall, 2007.

CRUZ, Juliana Cristina. **A ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA PARAMO FORTALECIMENTO DA CIDADANIA**. 68 pag. Monografia - Curso de Direito - Universidade Federal de Santa Catarina, Florianópolis, 2013.

DOLAN, A. **Engenharia Social**: Sans Institute. 2004.

FIGUEIREDO, Lucas. **Ministério do Silêncio: A história do serviço secreto brasileiro de Washington Luís a Lula (1927-2005)**. Rio de Janeiro: Record, 2005.

FONSECA, Paula F. **Gestão de Segurança da Informação: O Fator Humano**. 2009. 16 f. Monografia Especialização– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: https://www.academia.edu/33539394/Gest%C3%A3o_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_O_Fator_Humano. Acesso em: 12 jun. 2023.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6 ed. São Paulo: Atlas 2011.

GONÇALVES, Paulo Teles. **Contrainteligência e sua abrangência no brasil**. 35 pag. Monografia - Especialista em Inteligência de Segurança - Universidade do Sul de Santa Catarina, Campos Novos, 2019.

HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires. **Referenciais Básicos para a Capacitação de Profissionais de Inteligência de Segurança Pública no Brasil**. Revista Brasileira de Inteligência, p. 142, 2017.

HINTZBERGEN, Jule et al. **Fundamentos da Segurança de Informação baseado na ISO 27001 e 27002**. 3ª edição revisada. Rio de Janeiro: Brasport. 2015.

HORTA, Rodrigo Otávio A gestão da segurança institucional na Administração Pública. **Boletim Científico ESMPU**, p. 277–293, 2016.

IFSP. **Perguntas Frequentes - Cursos de Extensão**. São Paulo, 2020. Disponível em: https://www.ifsp.edu.br/images/prx/NormasManuais/faq_cursos.pdf. Acesso em: 15 jun. 2023.

IIA. **As três linhas de defesa no gerenciamento e controle de riscos eficazes**. Position Paper, 2013

ISONI, Miguel Maurício. **Comunidades Mediadas pela Internet: fatores de sucesso**. Tese de Doutorado em Ciência da Informação. Marília/SP: Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP), 2009. 174 fls

JUNIOR, Arnaldo Godoy. **A EVOLUÇÃO HISTÓRICA DA ATIVIDADE DE INTELIGÊNCIA NO BRASIL UM APRIMORAMENTO NA INTEGRAÇÃO ENTRE AS INSTITUIÇÕES**.35 pag. Artigo - Especialista em Altos Estudos em Defesa - Escola Superior de Guerra, Brasília, 2020.

JUNIOR, Arnaldo Godoy. **A evolução histórica da atividade de inteligência no brasil um aprimoramento na integração entre as instituições**.35 pag. Artigo - Especialista em Altos Estudos em Defesa - Escola Superior de Guerra, Brasília, 2020.

KARLOVA, Natascha A.; FISHER, Karen E. **A social diffusion model of misinformation and disinformation for understanding human information behaviour**. Information Research, v. 18, n. 1, p. 1-12, 2013.

KIZZA, J. M. **Guide to Computer Network Security**. New York: Springer International Publishing, 2017

LABFIN PROVAR. Entenda o que é e quem pode fazer um curso de extensão. **FHA BUSINESS SCHOOL**, São Paulo, ano 2019, p. 1 - 2, 28 out. 2019. Disponível em: <https://labfinprovarfia.com.br/blog/curso-de-extensao/>. Acesso em: 15 jun. 2023.

MARANHÃO. **Constituição do Maranhão**. São Luís, 05 de Out. 1989. Disponível em: <https://www2.senado.leg.br/bdsf/item/id/70443> Acesso em: 4 jun. 2023

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. 7. ed. São Paulo: Atlas, 2018. 373 p.

MARQUES, Eduardo. **Os mecanismos relacionais**. Revista Brasileira de Ciências Sociais, vol. 22, nº 64, p. 157-161. Jun. 2007.

MITNICK, K.; SIMON, W. L. **The art of deception: controlling the human element of security**. 1. ed. Indianápolis: Wiley Publishing Inc., v. 1, 2002.

NOVELLINO, V. N. Análise da lei nº 9.883/99 como marco jurídico da atividade de inteligência de estado no brasil (necessidade de novo marco regulatório para inteligência de estado no brasil). **Revista Brasileira de Inteligência**, p. 136, 2020

OAB. **Segurança Corporativa - Guia de Referência**. 1º Ed. São Paulo. 2015. Disponível em: https://www.oabsp.org.br/comissoes2010/gestoes2/2016-2018/direito-eletronico-crimes-altatecnologia/cartilhas/GuiaSegCorp_OAB_042015_final_cs.pdf. Acesso em: 05 jun.2023.

OLIVEIRA, M. CICLO PDCA - **O Método para solução de problemas: Guia prático das 4 fases e 8 etapas do PDCA**. Amazon Digital Services LLC - KDP Print US, 2019. 26 pag

PACHECO, José Edgar Cardoso de Sá. **Gestão da Segurança Organizacional numa Unidade Operacional de Saúde**. Dissertação de Mestrado - Universidade do Porto, Porto, 2017.

PROMON BUSINESS & TECHNOLOGY REVIEW. **Segurança da informação: um diferencial determinante na competitividade das corporações**. São Paulo, 2005.

RAZZETTI, E.A. **Auditing Organizational Security**. Defense AT&L Magazine - Defense Acquisition University, 2017.

RIBEIRO, Marcelo Martins. **Planejamento de desenvolvimento de segurança orgânica: uma proposta para as unidades do CBMMA**. Animaeducação, 2019. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/11861>. Acesso em 30 mai. de 2023.

ROSS, R. L. et al. **NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**. Maryland: National Institute of Standards and Technology, 2019.

SEMOLA, Marcos. **Gestão da Segurança da Informação - Uma Visão Executiva**. São Paulo, Campus.2014.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. ed. rev. e atual. São Paulo: Cortez, 2007.

SILVEIRA, Luís Felipe Ferreira. **O Planejamento de Contraineligência**.65 pag. Monografia - Especialista em Ciências Militares - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019.

SPITZNER, L. Securing the Human, SANS. 2014. Disponível em: <https://securingthehuman.sans.org/media/resources/presentations/STH-PresentationSecuringTheHuman.pdf>. acesso em: 27 mai. 2023.

TALBOT, J., E M. JAKEMAN. **Security Risk Management Body of Knowledge**. Hoboken, New Jersey: John Wiley & Sons, Inc., 2009

WAKE, T. **Princípios básicos de segurança para pequenas e médias empresas**. 2011. Disponível: <http://www.halkynconsulting.co.uk/securityresources/downloads/Security-Guide-for-Small-Medium-BusinessesV1.pdf>. acesso em 11 jun. 2023.

WATSON, G.; MASON, A.; ACKROYD, R. **Social engineering penetration testing: executing social engineering pen tests, assessment and defense**. Oxford: Elsevier, 2014.

WHITMAN, M. E.; MATTORD, H. J. **Princípios de Segurança da Informação**. São Paulo: Cengage Learning, 2018.

APÊNDICES

APÊNDICE A: QUESTIONÁRIO UTILIZADO NA PESQUISA

- 1) Qual o seu ano na ABMJM?
 - a) 1º Ano b) 2º Ano c) 3º Ano
- 2) Qual a sua idade?
 - a) entre 18 a 21 anos
 - b) entre 22 a 28 anos
 - c) entre 29 a 35 anos
 - d) mais de 35 anos
- 3) Qual seu nível de conhecimento no que diz respeito a aspectos de Segurança no Pessoal?
 - a) Muito bom b) bom d) regular e) ruim ou péssimo
- 4) Na sua opinião, abordar aspectos de Segurança para o Pessoal na ABMJM é:
 - a) Muito Importante b) Importante c) Pouco Importante d) Irrelevante
- 5) O senhor conhece as principais normas e legislações que tratam aspectos de Segurança no Pessoal (efetivo)?
 - a) sim b) não
- 6) A ABMJM promove algum programa de conscientização que enfatize a segurança de Pessoal?
 - a) sim b) não
- 7) Como o Senhor(a) considera a importância de se ter programas de conscientização dos colaboradores em relação a Segurança de Pessoal?
 - a) muito relevante b) relevante c) pouco relevante d) nada relevante
- 8) Quantas vezes o senhor(a) soube de incidentes dentro ou fora da UBM que comprometeu a Segurança de Pessoal, ou seja, de algum integrante do CBMMA,

como por exemplo: situações de insegurança em ocorrência, perda de materiais e equipamentos por descuido da guarnição, bombeiros acometidos de assaltos ou golpes por falta de atenção em aspectos de segurança e etc...?

a)01 b)02 c)03 d)04 e) várias vezes f) Nenhuma

9) Caso afirmativo a resposta anterior, que tipo de incidente teve conhecimento?

10) O papel de militares mais antigos na promoção da cultura de segurança de pessoal na ABMJM é

a) Muito Importante b) Importante c) Pouco Importante d) Irrelevante

11) A ABMJM realiza avaliações periódicas da efetividade do programa de segurança de pessoal?

a) sim b) não

12) Qual o seu nível de conhecimento acerca de boas práticas de segurança na internet, uso de redes sociais e salvaguarda de informações sensíveis?

a) Muito Bom b) Bom c) Regular d) Ruim ou péssimo

APÊNDICE B: CARTILHA DE CONTRAINTELIGÊNCIA PARA BOMBEIROS MILITARES

CARTILHA DE CONTRAINTELIGÊNCIA PARA BOMBEIROS MILITARES



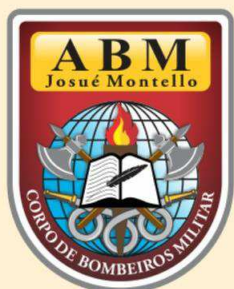
O PROJETO

CAD BM/3 355 João
Gestor do Projeto

Esta cartilha foi criada para conscientização e orientação em boas práticas de contrainteligência para a promoção da segurança de pessoal dos cadetes da Academia de Bombeiros Militar Josué Montello (ABMJM). A cartilha conta com conteúdo de referência do Programa Nacional de Proteção de Conhecimentos Sensíveis e tem a supervisão do Major QOCBM Paulo Rogério dos Santos Ribeiro, subcomandante da ABMJM.

ÍNDICE

- 04** Contraineligência
- 05** Engenharia Social
- 06** Reuniões Sensíveis
- 07** Uso do aparelho celular
- 08** Segurança na Internet



CAD BM/3 355 João

Gestor do projeto

Contrainteligência

A contrainteligência é uma atividade fundamental para a proteção de informações sensíveis e ativos pessoais. Como bombeiros militares, vocês possuem informações confidenciais que podem ser alvo de ameaças externas e internas. Portanto, é importante se familiarizarem com conceitos básicos de contrainteligência e adotarem boas práticas de segurança para protegerem a si mesmos e informações não autorizadas.

A contrainteligência é o conjunto de medidas que visam proteger informações sensíveis e ativos pessoais de ameaças internas e externas. Na segurança de pessoal tem o objetivo assegurar comportamentos adequados à salvaguarda de dados e conhecimentos sigilosos.

ENGENHARIA SOCIAL

A engenharia social é uma técnica utilizada para enganar, manipular ou explorar a confiança das pessoas, sem recorrer à violência física. Essa forma de ataque tem como objetivo induzir a vítima a realizar ações prejudiciais por conta própria, como revelar informações sensíveis ou efetuar transferências financeiras para desconhecidos.

A engenharia social pode ser aplicada tanto em situações pessoais como em contextos profissionais.

Boas Práticas:

1 - Desconfiar: Pense no que está fazendo, não clique em links e anexos sem uma comprovação. Desconfie ao passar informações.

2- Verifique: Saiba com quem está falando, solicite a identificação e comprove com um militar de confiança ou mais antigo caso ainda haja dúvidas.

3 - Limite Informações: Dificulte a disponibilidade de informações pessoais e profissionais em redes sociais. Conheça quais informações pessoais são de livre acesso. Não demonstre empatia com desconhecidos que usem dessas informações.

4- Conheça o que pode ser compartilhado: Consulte normas e militares mais antigos e autorizados sobre quais informações institucionais podem ser compartilhadas. Seja cuidadoso ao divulgar suas informações pessoais.

5 - Alerta

Ao possuir desconfiança que foi alvo de engenharia social, comunique imediatamente seu superior hierárquico e apresente os fatos e informações repassadas.





REUNIÕES SENSÍVEIS

Em reuniões um serie de conteúdos podem ser abordados, assim como informações que devem ser bem tratadas e avaliadas.

Tome a seguintes posturas:

- 1- Reconheça se há necessidade de você conhecer o assunto discutido, caso contrário, solicite sua retirada.
- 2 - Caso permaneça na reunião, trate apenas do assunto pautado ou autorizado pelo responsável pela reunião.
- 3 -Limite o uso de aparelhos eletrônicos ao estritamente necessário, caso possível, desligue.
- 4 -Reconheça os possíveis interessados nos temas tratados na reunião.
- 5 - Saiba das medidas e consequências de eventual vazamento de informações sobre você e a instituição.
- 6 - Sempre informe se você possui a capacidade de guardar de forma segura as informações sensíveis compartilhadas em qualquer momento, antes, durante ou após a reunião.



USO DO APARELHO CELULAR

O celular é um dos principais meios de acesso à internet, da mesma maneira que é porta de entrada para ameaças, com isso é importante o uso do aparelho de maneira segura.

Tome as seguintes posturas:

- 1- Evite wi-fi de ambientes públicos, inclusive aeroportos
- 2 - Evite carregar seu celular em computadores e carregadores públicos via cabos USB.
- 3 - Desligue Wi-fi, bluetooth e localização quando não estiverem em uso.
- 4 -Desative notificações na tela.
- 5 - Habilite o bloqueio automático de tela.
- 6 - Não compartilhe celular com pessoas que não precisam saber o que você possui instalado nele.
- 7 - Desconfie de ligações suspeitas de desconhecidos que tentem levantar informações pessoais e institucionais.
- 8 - Desconfie do mesmo tipo de ligação para mais de uma pessoa da instituição.

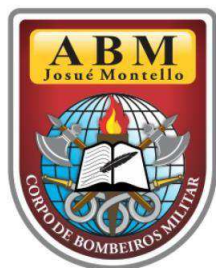
Segurança na Internet

Recomendações para a proteção de suas informações e material instrucional no uso da internet:

- 1 - Tome consciência que as informações compartilhadas irão além do destinatário original.
- 2 - Como cadete você representa sua instituição, pense cuidadosamente sobre o que pública, saiba se tem autorização para publicar determinadas informações.
- 3 - Não use seu e-mail institucional para uso de sites que não possuem qualquer ligação com o trabalho da instituição.
- 4 - Verifique cuidadosamente imagens que irá publicar, certifique que nenhuma informação será vazada involuntariamente.
- 5 - Sempre pense se sua exposição a rede está dentro do necessário.
- 6 - Evite abrir mensagens sem identificação ou se houver suspeita de endereço falso.
- 7 - Desconfie de ofertas financeiras vantajosas na compra de produtos. Não realize transações financeiras em sites que você não conheça a segurança.
- 8 - Não acesse e-mails de anúncios (Spam)
- 9 - Segmentar seus perfis em rede com contas, nomes e senhas diferentes. Se possível, separe seu perfil pessoal do profissional.

Estas ações além de protegerem o ambiente institucional, auxiliam na segurança da informação, na gestão corporativa e de pessoas





2023

Academia de Bombeiros Militar
Josué Montello

**“CONCENTRE-SE NO PONTOS
FORTES, RECONHEÇA AS
FRAQUEZAS, AGARRE AS
OPORTUNIDADES E PROTEJA-SE
CONTRA AS AMEAÇAS.” SUN TZU**

REFERÊNCIA:

BRASIL. ABIN. Programa Nacional de Proteção do Conhecimento Sensível: Boas Práticas. Brasília, 2022.

