

COMBATE AO CIBERCRIME: aspectos da formação e preparo do policial militar no Estado de Goiás

COMBAT CYBERCRIME: aspects of training and preparation of military police in the State of Goiás

João Marcos Lopes da Silva*
Vânia Spindola Arantes da Silva**

RESUMO

O combate ao cibercrime envolve diversos aspectos aos quais o agente de segurança pública deve ter conhecimento para proteger a sociedade contra os criminosos. Dessa forma o objetivo dessa pesquisa é avaliar se o policial militar recebe instrução específica para investigação e combate aos cibercrimes nas disciplinas ministradas nos cursos segurança pública. O que justifica a pesquisa sobre esse tema é o crescimento dessa prática delituosa, e a necessidade de o policial militar estar preparado para atuar no auxílio às polícias investigativas. Os métodos e técnicas utilizados no desenvolvimento da pesquisa se deu através da coleta de dados em um formulário estruturado, que buscou conhecer sobre a formação do policial militar nos cursos de Pós-Graduação em Segurança Pública da Academia da Polícia Militar de Goiás. Obtendo-se como resultado o desconhecimento dos agentes sobre os aspectos que envolve esse tipo de crime, e a necessidade de aplicar na aprendizagem, disciplinas que permita ao policial militar atuar com eficácia no combate aos cibercrimes.

Palavras-chave: Cibercrimes. Formação Policial Militar. Matrizes Curriculares.

ABSTRACT

Combating cybercrime involves several aspects that public security agents must be aware of to protect society against criminals. Therefore, the objective of this research is to evaluate whether military police officers receive specific instruction to investigate and combat cybercrimes in the subjects taught in public security courses. What justifies research on this topic is the growth of this criminal practice, and the need for military police officers to be prepared to act in aid of the police. The methods and techniques used in the development of the research were carried out through the collection of data in a structured form, which sought to learn about the training of military police officers in the Postgraduate courses in Public Security at the Military Police Academy of Goiás. Obtaining As a result, agents are unaware of the aspects involved in this type of crime, and the need to apply disciplines in learning that allow military police officers to act effectively in combating cybercrimes.

Keywords: Cybercrimes. Military Police Training. Curricular Matrices.

* Aluno no Curso de Pós-Graduação em Segurança no Pública, Turma N 6ª Cia, do Comando de Polícia Militar do Estado de Goiás (CAPM). E-mail: marcos-lsxd@hotmail.com.

** Professor orientador, Especialista em Criminologia e Segurança Pública, Comando da Academia da Polícia Militar de Goiás, Goiânia-GO, 18/12/2023.

1 INTRODUÇÃO

Os cibercrimes são atividades criminosas praticadas em ambientes virtuais através de equipamentos como computadores, celulares, entre outros. Uma pesquisa publicada no Jornal Opção em 2022, apontou um aumento de 89% de crimes cibernéticos, e uma das razões apontadas pelo advogado Caio Mendes, seria a dificuldade de identificação do infrator e o fato de haver pena branda na legislação brasileira. (FERREIRA, 2022)

De acordo com Martins (2010) a Polícia Militar pode atuar repressivamente nas operações de rastreamento, prisão em flagrante, registro do boletim de ocorrência, acionamento da perícia técnica, busca e apreensão de equipamentos, materiais e objetos utilizados na prática do crime, por meio de mandado judicial. Segundo o autor, também pode atuar na prevenção, com presença constante nos locais abertos como *Lan House* e *Cibercafés* para reprimir essa prática.

Martins (2010), em sua pesquisa no Estado de Minas Gerais, mostrou que a maioria dos policiais não tem nenhum conhecimento sobre o tema, e que além da falta de conhecimento e qualificação, também falta equipamentos e materiais para treinamento.

E a partir disso, surgiu a seguinte questão: Os policiais militares do Estado de Goiás recebem treinamento nessa área nos cursos de formação para atuar frente aos crimes praticados em ambiente virtual?

Nesse sentido essa pesquisa justifica-se devido ao crescimento dessa prática delituosa, onde espera-se que o policial militar esteja preparado para atuar no auxílio às polícias investigativas no combate ao cibercrime e ainda ampliar o leque de discussões sobre a temática nos cursos preparatórios para os novos acadêmicos e sobre as disciplinas específicas relacionadas ao cibercrime.

O principal objetivo deste trabalho é avaliar se o policial militar recebe instrução específica para investigação e combate aos cibercrimes nas disciplinas ministradas nos cursos segurança pública. Os objetivos específicos deste artigo são:

- a) discorrer sobre a punibilidade dos crimes praticados em ambiente virtual na legislação atual;
- b) descrever estrutura e a importância da formação policial; e
- c) analisar as grades curriculares dos cursos ofertados em Segurança Pública.

A presente pesquisa, inicialmente de caráter bibliográfico terá como fonte obras publicadas entre 2003 e 2023, em meio eletrônico. Servirá de base de busca, sites como o Google Acadêmico, o Scielo Brasil e o acervo digital da Secretaria de Segurança Pública do

Estado de Goiás, entre outros.

E também, como pesquisa documental através da coleta de dados em sites que ofertam cursos na área de Segurança Pública, como o acervo da Secretaria de Segurança Pública, da Secretaria Nacional de Segurança Pública, entre outras plataformas digitais, buscando ainda, avaliar os aspectos abstratos e a classificação e interpretação das informações obtidas com a coleta de dados, a pesquisa será de natureza quali-quantitativa.

A pesquisa de campo ocorrerá por meio de coleta de dados, utilizando-se um formulário com questões de múltipla escolha enviado via WhatsApp para os grupos da Polícia Militar de Goiás.

2 REVISÃO DE LITERATURA

Devido ao crescimento dos crimes praticados em meio virtual faz-se necessário compreender os aspectos que envolve esse tipo de crime e como a Polícia Militar Ostensiva está preparada para agir no combate a essa prática. Essa seção discorrerá sobre o uso da internet para fins ilícitos, sobre a formação e o preparo do policial militar na carreira e ainda sobre a inserção de disciplinas específicas na grade curricular dos cursos de formação policial.

2.1 A INTERNET USADA PARA FINS ILÍCITOS

Desde a criação dos computadores digitais na década de 40, muitas mudanças surgiram ampliando o leque de possibilidades de uso desse equipamento que inicialmente foi criado para facilitar cálculos matemáticos, e, após o surgimento da internet, é utilizado como ferramenta de comunicação global.

Cada vez mais as pessoas se relacionam através do mundo digital. O cotidiano depende da internet para questões diversas como compras com cartões de crédito e débito ou pagamentos via pix para a aquisição de bens e serviços. Essa forma constante de interação, acarreta preocupação das organizações sociais como o poder judiciário, a imprensa e a sociedade de forma geral, em relação a proteção de dados pessoais e o sigilo do conteúdo das comunicações privadas. (FERREIRA, 2021)

O surgimento da internet no Brasil, na década de 80 tornou-se o principal meio de comunicação e teve um crescimento gradativo, principalmente devido as condições

socioeconômicas dos brasileiros. De acordo com Correa (2013) em 2007 com 49 milhões de usuários e em 2011 com um aumento de 51% de usuários acima de 16 anos. Queiroz (2021) afirma que de acordo com as pesquisas do Instituto Brasileiro de Geografia e Estatística em 2019 o crescimento do acesso à internet no Brasil cresceu muito apresentando um aumento de domicílios conectados em 82,7%.

Para Carvalho (2006, p. 154) “Internet não é pura e simplesmente uma rede técnica, feita de hardware e software. Ela é uma rede sociotécnica, ou, dito de outra forma, um enredamento indissociável de ciência, tecnologia e sociedade”, embora surgida de uma idealização subjetiva e abstrata, trouxe resultados hoje materializados na forma de viver de cada indivíduo com computadores móveis, televisão digital, entre outros.

Sendo a internet um mundo imaterial e imensurável é também definido como ciberespaço, e Carvalho (2006) cita a *Declaração de Independência do Ciberespaço* representada por Barlow (1996): “Ó Governos do Mundo Industrial, esgotados gigantes de carne e aço, eu venho do ciberespaço, a nova morada da mente. [...] O ciberespaço não se situa dentro de suas fronteiras. [...] (BARLOW, 1996 *apud* CARVALHO, 2006, p. 218)

Embasado no trecho citado, Carvalho (2006) descreve o ciberespaço como um elemento impalpável que através de um conjunto de hardware e software determinará o comportamento dos seus usuários. Sendo crime, qualquer ato praticado nessa esfera, quando se invade dados pessoais ou sigilosos de pessoas ou empresas com o objetivo violar os direitos de outro em benefício próprio. (QUEIROZ, 2021)

Legalmente falando, a internet sempre foi regida por códigos, mesmo sendo conhecidos por poucos, porém, quanto mais se expande o comércio eletrônico, novas regras de uso surgem para proteger os usuários. Entretanto, devido as frequentes mudanças no espaço virtual, o Direito Penal brasileiro enfrenta dificuldades em legislar sobre essa temática, e isso contribui para o aumento consideravelmente da incidência de crimes praticados por indivíduos que se aproveitam das fragilidades do sistema legal. (QUEIROZ, 2021)

Na legislação temos, por exemplo, Decreto-Lei 2.848/40 (Código Penal Brasileiro); a Constituição Federal de 1988; a Lei 10.406/2002 (Código Civil Brasileiro); e, a Lei 12.965/2014, também intitulada “Marco Civil da Internet”, que veio estabelecer os princípios, garantias, direitos e deveres para o uso da internet no Brasil, oferecendo mecanismos aplicáveis aos atos ilícitos cometidos no Brasil.

O Código Penal, assim como o Código Civil e a Constituição Federal, não tratam especificamente dos crimes virtuais, porém enquadra esses crimes como estelionato, formação de quadrilha, chantagem, extorsão, dentre outros. Tanto a Constituição Federal quanto o

Decreto-Lei 2.848/40 do Código Penal, em seu art. 1º decreta que “não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.” (BRASIL, 1940, p. 01).

Antes do Marco Civil da Internet, foi promulgada em 2012, a primeira lei a tratar mais especificamente os crimes cibernéticos. A Lei 12.737/12, que ficou conhecida como “Lei Carolina Dieckmann”, que altera o Decreto-Lei 2.484, de 7 de dezembro de 1940 do Código Penal. O artigo 154-A, sobre invasão de dispositivo informático, regimenta que:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 2012, p. 01)

Ferreira (2021) afirma que essa lei apresenta falhas, e acredita que isso se deu devido à imposição da mídia e da sociedade, acelerando sua aprovação. Segundo a autora, dentre as falhas observadas nessa lei, está o fato de que a invasão ocorrida em dispositivo sem um mecanismo de segurança, como senha, antivírus ou firewalls, não configura crime de invasão, e consequentemente não cabe punição ao autor da ação. Outra situação livre de punição acontece “quando um colega de trabalho compartilha o computador com outro e descobre informações ou fotos deste e as divulga. Nessa situação, mesmo que existisse o mecanismo de segurança no computador do trabalho, o agente não teve que ultrapassá-lo”. (FERREIRA, 2021, p. 21)

Devido a essas falhas, as discussões levaram a criação da Lei 14.155, que foi sancionada em 21 de maio de 2021. Essa lei altera o Decreto-Lei nº 2.848/40, tornando mais graves os

crimes de invasão de aparelhos eletrônicos ou invasão virtual. A Lei 14.155/21 trouxe mudanças na tipificação dos crimes de invasão de dispositivos, conectados ou não à internet como furto qualificado e estelionato. Furto qualificado quando ocorre por meio eletrônico invadindo dispositivos de segurança, ou utilizando programa malicioso. E estelionato, quando a vítima, ao ser enganada, fornece informações por meio de redes sociais ou mesmo via telefônica. (BRASIL, 2021; BAPTISTA, 2021)

Principalmente dada a importância da internet e a sua utilização pelo comércio nos últimos anos, a criação das leis trouxe um avanço significativo, para reprimir essa prática que muitas vezes é usada para chantagear e extorquir os cidadãos. Conforme mostra Carvalho (2006, p. 219): “Agora, não apenas tornando esse ciberespaço livre como também criando condições para que a vida de seus ‘cibercidadãos’ fosse passível de uma regulação e controles jamais vistos anteriormente”

Entretanto, acredita-se que o Brasil ainda não alcançou uma legislação adequada, o que acarreta ainda insegurança dos usuários. A questão jurídica ainda não foi esgotada, requer muito debate e ajustes. São necessários mais investimentos em segurança e treinamento especializado dos agentes envolvidos.

2.2 INGRESSO E FORMAÇÃO NA CARREIRA MILITAR

Como instituição atuante no Brasil desde o século XIX, a Polícia Militar passou por diversas mudanças. Detentora de poder no exercício da função, nem sempre foi intitulada como Polícia Militar, mas como Guarda Real de Polícia em 1809, Força Policial em 1858, Companhia de Polícia de Goiás em 1892, Batalhão de Polícia de Goiás em 1910, Força Pública Militar de Goiás em 1930, Polícia Militar de Goiás em 1935, e Polícia Militar do Estado de Goiás em 1988, dentre outras mudanças também ocorridas. Mudança não apenas na titulação desse órgão, mas também mudanças estruturais e legais devido as transformações do cenário mundial. (PEREIRA, 2013)

A carreira de Policial Militar exige que o interessado possua curso superior, e além da aprovação no processo seletivo da PMGO, deverá ingressar em cursos sequenciais para elevar o nível cultural e profissional do ingressante propiciando ao mesmo, o domínio de conhecimentos sistematizados, além de específicos no trato à proteção social. (PEREIRA, 2013)

A preparação do policial militar surgiu da necessidade deste apreender técnicas,

procedimentos e preceitos para melhor realização de suas obrigações. E nesse sentido, espera-se que possa garantir que os direitos de cada cidadão sejam respeitados, acarretando a necessidade de aperfeiçoar cada vez mais o ensino oferecido ao policial militar no estado de Goiás. Nesse contexto, Souza (2003) explica que há diferenças entre ensino militar e o ensino policial militar:

O ensino militar é aquele ministrado nas escolas militares das Forças Armadas (Marinha, Exército e Aeronáutica). Como o objetivo precípua destas é a manutenção da paz e da soberania da nação, a formação é feita por meio de um currículo que enfatiza disciplinas relacionadas com o conflito armado convencional propriamente dito. O militar das Forças Armadas é preparado efetivamente para a guerra. Já o ensino policial militar é aquele ministrado nas escolas militares das polícias militares do Brasil, por exemplo, na Academia de Polícia Militar de Goiás. A finalidade essencial do currículo dessas escolas é preparar o policial militar para promover a segurança do cidadão, nas mais variadas circunstâncias que se apresentem. (SOUZA, 2003, p. 52)

Ou seja, o ensino militar prepara para a guerra propriamente dita, enquanto o ensino policial prepara o ingressante para atuar na prevenção e combate as infrações que ferem a segurança e o direito dos cidadãos.

Desenvolver uma formação profissional individual e coletivo é desafiador e requer diferentes habilidades como “capacidade de rápida adaptação a novas situações [...], autocontrole, bom senso, raciocínio rápido, cortesia, conhecimentos gerais e específicos e a necessária energia no enfrentamento de ocorrências.” (SOUZA, 2003, p. 52)

Nesse sentido, entende-se que o ensino precisa estar aberto as inovações impostas pelas constantes transformações, ampliando o leque de possibilidades no intuito de aperfeiçoar as técnicas de trabalho.

2.3 MATRIZES CURRICULARES E DISCIPLINAS ESPECÍFICAS PARA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

A formação do policial militar é caracterizada por um conjunto de conhecimentos teóricos e habilidades técnicas a serem desenvolvidas através de cursos na área de segurança pública. Esses cursos são desenvolvidos a partir da Matriz Curricular Nacional, criada pelo Ministério da Justiça, publicada em 2014. (SOUZA, 2020)

A Matriz Curricular Nacional é um conjunto normativo criado para orientar as ações na formação militar:

[...] um referencial teórico-metodológico para orientar as ações formativas - inicial e continuada - dos profissionais da área de segurança pública - Polícia Militar, Polícia Civil, Corpo de Bombeiros Militar, independentemente do nível ou da modalidade de ensino que se espera atender. Seus eixos articuladores e áreas temáticas norteiam, hoje, os mais diversos programas e projetos executados pela Secretaria Nacional de Segurança Pública (SENASP, 2014, p. 12).

Esse conjunto normativo tem como objetivo o desenvolvimento e a conduta moral e ética individual nas práticas profissionais e nos relacionamentos sociais.

Entretanto, de acordo com Souza (2020) a Matriz Curricular Nacional não é obrigatória e sim um conjunto de eixos formadores sugeridos pelo Ministério da Justiça, deixando a critério de cada instituição, quais e como serão trabalhados cada eixo na formação das disciplinas dos cursos oferecidos por esta. O conjunto estruturado de conteúdos que formam a matriz são conhecidos como eixos articuladores e deve contemplar aspectos do contexto social, histórico e político atual. (PEREIRA, 2013)

De acordo com Carneiro (2019) o conhecimento necessário em Segurança Pública é determinado por esse instrumento de gestão educacional e pedagógica. E Correa (2018) afirma que os cursos de formação, aperfeiçoamento, nivelamento e reciclagem de aprendizados moldam o perfil dos profissionais em segurança pública.

Pereira (2013) diz que a Matriz Curricular da Polícia Militar de Goiás, partiu de minuciosas discussões quanto a finalidade do curso:

[...] 1) O aluno recém-matriculado em curso revela comportamentos que deverão ser enriquecidos com as experiências proporcionadas pelo estabelecimento de ensino. Estas experiências, intencionalmente selecionadas constituem o currículo, no sentido do amplo deste termo. [...] Os Currículos precisam ser constantemente avaliados. As modificações a serem introduzidas são fruto de permanente observação e devem ser feitas dentro de uma sistemática de trabalho. (NORMAS PARA ELABORAÇÃO E REVISÃO DE CURRÍCULOS, 1987, p. 1 *apud* PEREIRA, 2013, p. 69).

É importante salientar que a Matriz Curricular dos cursos obrigatórios de formação em Segurança Pública, sofreram alterações ao longo dos anos, e algumas disciplinas entraram e saíram das grades, e nessa pesquisa, percebe-se que disciplinas especificamente voltadas ao conhecimento das técnicas aplicadas por ciberdelinquentes não foram contempladas, sendo interessante uma verificação mais aprofundada.

Na plataforma de ensino à distância da Secretaria de Gestão e Ensino em Segurança Pública (SEGEN), são oferecidos diversos cursos. Dentre os cursos ofertados consta:

a) *Inteligência Cibernética: Produção de conhecimento com segurança*, com 6h, esse curso é reservado apenas para profissionais de Inteligência por indicação das agências de

inteligência de cada Estado. Esse curso visa “apresentar o funcionamento do espaço cibernético (atividades realizadas pela internet, redes sociais, ferramentas de coleta, noções de Deep Web), além de assegurar aos profissionais de ISP os meios seguros para navegação em ambiente cibernético”. (FERNANDES, 2023, p. 01);

b) *Detecção de Fraudes Eletrônicas em Períodos de Crise*, com 15h. Curso destinado aos profissionais que integram o Sistema Único de Segurança Pública (SUSP).

Difundir informações sobre os principais golpes praticados em tempos de crise buscando realizar a prevenção de fraudes no meio cibernético, bem como, repassar ao profissional de segurança pública, a casuística e os caminhos para a mitigação dos efeitos danosos dessa modalidade delitiva em tempos de pandemia e oportunismo. (FERNANDES, 2023, p. 01);

c) *Crimes Cibernéticos – Noções Básicas*, com 60h. Também destinado aos profissionais integrados ao SUSP. Objetivando desenvolver competências relacionadas a investigação de cibercrimes, o curso aborda a tipologia do crime, as fases do processo de investigação e as leis pertinentes. (FERNANDES, 2023)

Os cursos acima citados são de curta duração e não consta nenhuma obrigatoriedade do ingressante na Polícia Militar frequentá-los.

A Secretaria Nacional de Segurança Pública (SENASP), em sua plataforma EAD oferece vários cursos autoinstrucionais em Segurança Pública, porém não consta em seus eixos temáticos nenhum curso na área pesquisada. A plataforma também oferece mestrados em segurança pública, conforme o Plano Anual de Ensino e Pesquisa (PAEP). O PAEP é uma ferramenta participativa, que permitiu a elaboração de conteúdos aperfeiçoados e direcionados às demandas. (FERNANDES, 2021)

A Secretaria de Segurança Pública de Goiás também oferece vários cursos, inclusive cursos de pós-graduação. Os ciclos 1, 2 e 3/2023 apresentam vários cursos como *Atendimento Policial ao TCO*, *Inteligência de Segurança Orgânica*, *Procedimento Operacional Padrão da Segurança Pública do Estado de Goiás*, *Registro de Ocorrências Prioritárias do Sistema RAI – ROP-RAI*, *Direitos e Garantias Fundamentais Aplicados à Prática Policial*. É possível observar que vários desses cursos tratam aspectos relacionados a investigações no espaço cibernético, porém nenhum deles trata o assunto com mais profundidade, ou seja, nenhum curso que aborde as técnicas de investigação de protocolos digitais, técnica forense digital em crimes cibernéticos.

Geralmente, os cursos que tratam especificamente essa temática, trabalham disciplinas como algoritmos e programação estruturada; criptografia; lógica computacional; linguagem de

programação; computação em nuvem; programação para redes; privacidade e proteção de dados.

O quadro 1 lista as disciplinas trabalhadas no curso de Pós-Graduação em Segurança Pública da Academia da Polícia Militar de Goiás, porém não contempla nenhuma disciplina com enfoque nos conhecimentos sobre cibernética ou ciberespaços.

QUADRO 1 – Malha curricular do CFP

Nº	Disciplinas do Curso de Formação de Praças	Carga Horária	EaD
1.	Atendimento Pré-Hospitalar	20	
2.	Ciências Penais	40	
3.	Defesa Pessoal Policial	40	
4.	Direito Militar – Penal Militar e Processo Penal Militar	30	
5.	Direitos Humanos (*)	25	
6.	Educação Física Militar	60	
7.	Estágio de Prática Profissional I (***)	160	
8.	Estágio de Prática Profissional II (***)	500	
9.	Estudos de Polícia e Policiamento	25	
10.	Estudos de Violência e Criminalidade	30	
1.	História e Organização da PMGO	15	
12.	Identificação de Fraudes Veiculares (*)	20	
13.	Instrução Geral e Regulamentos Militares	25	
14.	Instrução Tática Individual	20	
15.	Legislação Institucional	30	
16.	Metodologia de Pesquisa Científica aplicada à Segurança Pública (*)	30	
17.	Operações de Choque	25	
18.	Ordem Unida	30	
19.	Policiamento Comunitário e Policiamento Orientado para o Problema	15	
20.	Policiamento e Fiscalização Ambiental	30	
21.	Policiamento e Fiscalização de Trânsito	30	
22.	Procedimento Operacional Padrão – Módulo EaD (**)	10	80
23.	Processo Penal aplicado à Segurança Pública	30	
24.	Registro de Atendimento Integrado (*)	15	
25.	Saúde Mental (*)	13	
26.	Saúde e Segurança Pública (**)	00	23
27.	Sistemas de Segurança Pública (**)	00	23
28.	Sistemas Informatizados	39	
29.	Técnica Policial Militar I	40	
30.	Técnica Policial Militar II	30	
31.	Técnicas de Direção Policial (*)	20	
32.	Termo Circunstanciado de Ocorrência	20	
33.	Tiro Policial	50	
34.	Trabalho de Conclusão de Curso	80	
35.	Uso Seletivo da Força (*)	20	
CARGA HORÁRIA DAS DISCIPLINAS ACADÊMICAS		1567	126
TOTAL		1693	

Fonte: Academia da Polícia Militar de Goiás, 2022.

(*) Estas disciplinas contêm cursos oferecidos pela Plataforma de Ensino a distância da SENASP ou da GEAD/SSPGO. Disciplina vinculada a atividades de ensino a distância.

(**) Disciplinas de ensino a Distância na Plataforma de ensino do CAPM, as quais podem ocorrer presencialmente.

(***) Disciplinas independente com nota atribuída pelas atividades policiais militares realizada no âmbito interno do Comando da Academia de Polícia Militar e no âmbito externo desenvolvidas pelo discente em atividades práticas de polícia ostensiva e preservação da ordem pública. As atividades dos discentes devem ser devidamente registradas no Sistemas Informatizados da Secretaria de Segurança Pública.

Segundo Carneiro (2019, p. 17) “os agentes de Segurança Pública em especial os Policiais Militares que atendem diretamente o público precisam ter diferentes saberes, por se tratar de uma profissão multidisciplinar, adquirindo novas habilidades e competências para sua atuação cotidiana”. E com o aumento de crimes praticados no ciberespaço, percebe-se a importância de conhecimento nessa área.

3 METODOLOGIAS

A pesquisa bibliográfica de acordo com Minayo (2001) coloca o pesquisador e os autores num diálogo sobre o tema de interesse do pesquisador. Dalberio e Dalberio (2009, p. 167) complementa que “o pesquisador deve tomar cuidado com a fidedignidade e validade científica das informações sob o risco de incorrer em possíveis incoerência e contradições causadas por material de baixa credibilidade”. Nesse sentido, observou-se onde foi publicado e se houve supervisão de especialista, mestre ou doutor no trabalho publicado.

A busca de fontes bibliográficas para a pesquisa deu-se em acervos digitais da Secretaria de Segurança Pública, Revista Brasileira de Estudos de Segurança Pública (REBESP), Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), e plataforma digital do *Scientific Electronic Library Online* (SCIELO Brasil), e ainda em documentos como Leis e Decretos publicados nos sites do Governo Federal.

Teve como palavras-chave na busca de fontes: Crimes cibernéticos, ensino militar, formação policial militar, matriz curricular, internet e fins ilícitos. O que levou a obras publicadas por autores como: Carvalho (2006), Pereira (2013), Ferreira (2021), Queiroz (2021), Ferreira (2022), Souza (2020), Souza (2003), Carneiro (2019), dentre outros que servirão de base para o estudo das abordagens que envolvem o tema escolhido.

Ainda quanto aos métodos, trata-se de uma pesquisa qualitativa, porque busca compreender os aspectos subjetivos de uma organização social, observando as diferenças entre o mundo social e o mundo natural. (MINAYO. 2001)

Para a pesquisa de campo serão coletados dados através de um formulário com oito questões de múltipla escolha. O formulário será enviado via WhatsApp os grupos da Polícia

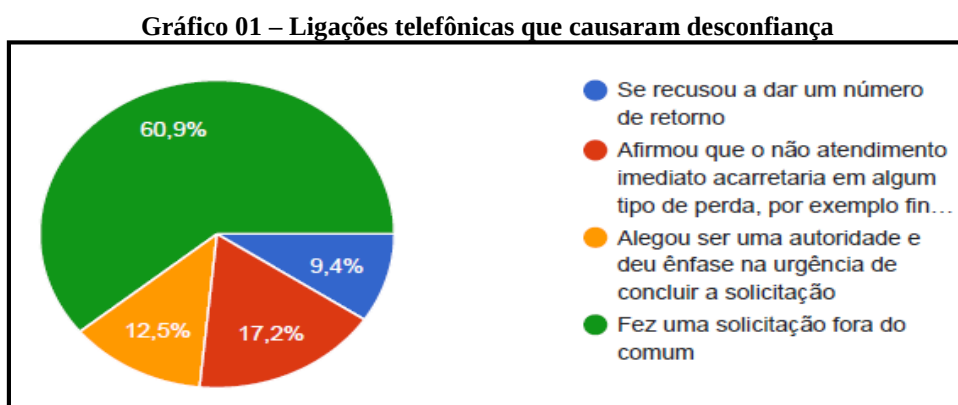
Militar de Goiás, lotados em Goiânia. Os indivíduos respondentes não serão identificados na pesquisa, apenas as respostas serão utilizadas para chegar a uma conclusão sobre a problemática levantada. Dos formulários devolvidos serão tabulados os dados dos primeiros formulários que retornarem devidamente preenchidos.

O artigo será distribuído em seções, sendo: resumo, introdução, revisão de literatura, metodologia, resultados e discussões, considerações finais, e uma lista com as obras dos autores pesquisados para a construção do trabalho.

4 RESULTADOS E DISCUSSÕES

A arte de enganar, de ludibriar é uma indústria que cresce dia a dia. Mitnick (2003, p. 06) afirma que a “engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação” diante da realidade cibernética hoje estamos sujeitos a cair em todos os tipos de golpes. Essa pesquisa tenta provar, entre outras coisas a nossa vulnerabilidade e a necessidade proteção de agentes como os policiais militares.

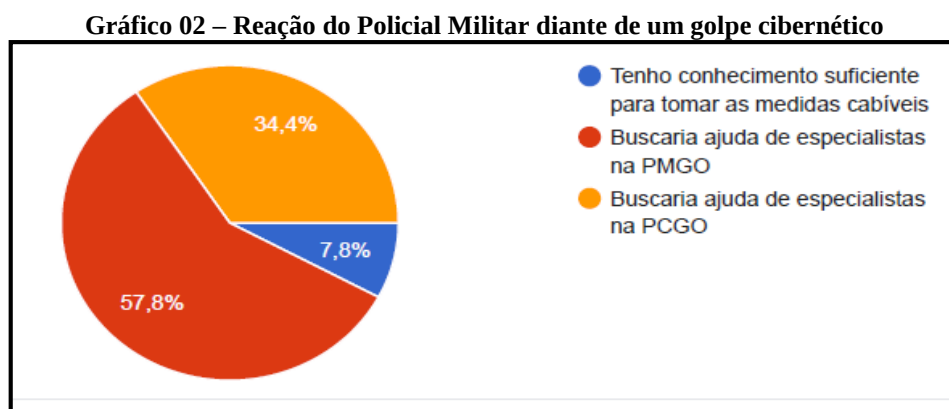
Após o envio dos formulários, retornaram 64 devidamente preenchidos, e os dados tabulados apontaram que 60,9% dos entrevistados já se depararam com ligações telefônicas suspeitas, devido a uma solicitação fora do comum, 17,2% receberam ligações em que a pessoa afirmava que o não atendimento imediato acarretaria algum tipo de perda; 12,5% afirmaram que receberam ligações de alguém alegando ser uma autoridade dando ênfase na urgência de concluir a solicitação por ele imposta; e 9,4% receberam ligação de alguém se recusando a dar um número de retorno, como relatado por Mitnick (2003). O Gráfico 01, demonstra nossa vulnerabilidade diante de agentes de má fé:



Fonte: Elaborado pelo autor (2023)

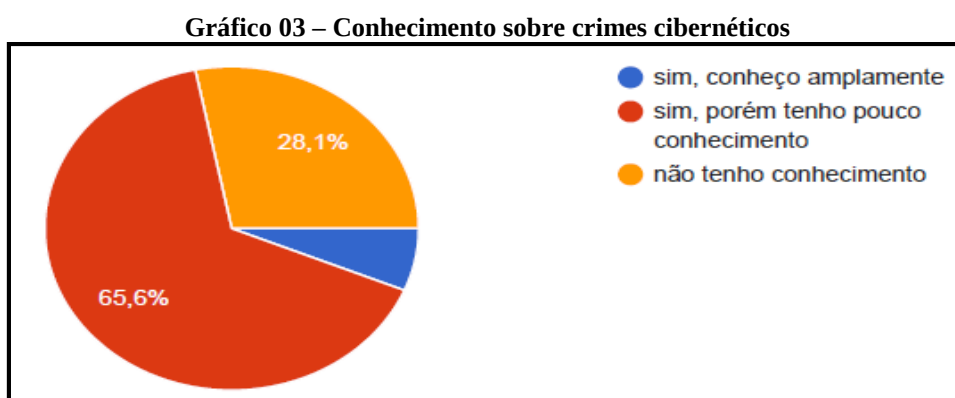
Ao questionar os entrevistados: Se você sofresse um golpe cibernético, como reagiria? 57,8% afirmaram que buscariam ajuda de especialistas da Polícia Militar de Goiás, outros 34,4% acreditam que a melhor opção é buscar ajuda da Polícia Civil, e nesse caso, percebe-se que provavelmente essa resposta recai sobre o poder investigativo da Polícia Civil. Apenas 7,8% afirma ter conhecimento suficiente para tomar as medidas cabíveis.

O Gráfico 02 mostra que a maioria dos policiais militares de Goiás não tem preparo e conhecimento suficiente para se proteger, o que pode ser observado pela Matriz Curricular do curso de Especialização em Segurança Pública, que observamos no Quadro 01. Nesse não consta disciplinas específicas que agregue conhecimento suficiente ao agente policial para reagir diante de situações como a apontada na questão 02. Situação essa corroborada por Carneiro (2019) ao afirmar a necessidade de ampliar os conhecimentos multidisciplinares.



Fonte: Elaborado pelo autor (2023)

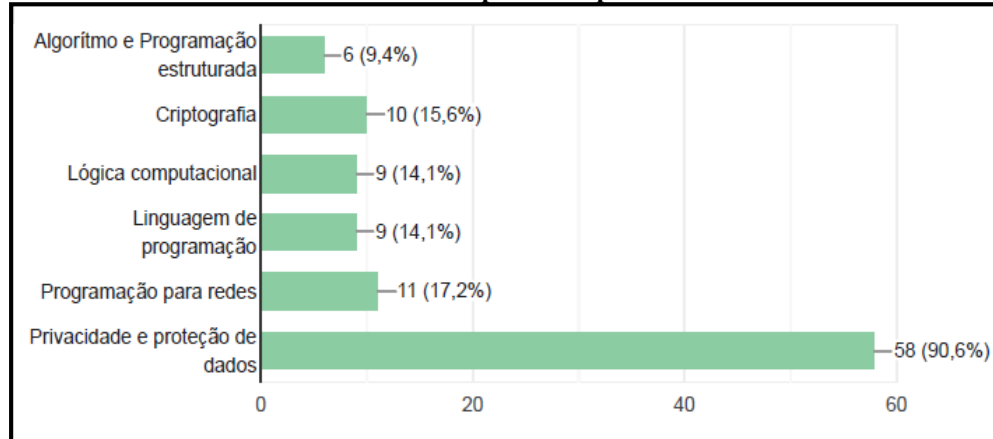
Os crimes cibernéticos, apesar de ocorrerem desde o evento dos computadores e principalmente das redes de internet, muitos ainda têm pouco ou nenhum conhecimento sobre o tema, como demonstrado no Gráfico 03, onde 65,6% dos respondentes afirmaram que tem pouco conhecimento e 28,1% não tem conhecimento algum.



Fonte: Elaborado pelo autor (2023)

Para combater os crimes cibernéticos são necessários alguns conhecimentos específicos dentre eles: Privacidade e proteção de dados, informados por 90,6% dos questionados, como um conhecimento importante. 17,2% informaram ter conhecimento em programação para redes; 15,6% têm conhecimento em criptografia; 14,1% têm conhecimento em lógica computacional e linguagem de programação e apenas 9,4% têm conhecimento na área de algoritmo e programação estruturada. Ressaltando que para essa questão o entrevistado poderia apontar mais de um dos conhecimentos citados, ou seja, entre os 64 respondentes obteve-se 103 respostas. Veja Gráfico 04:

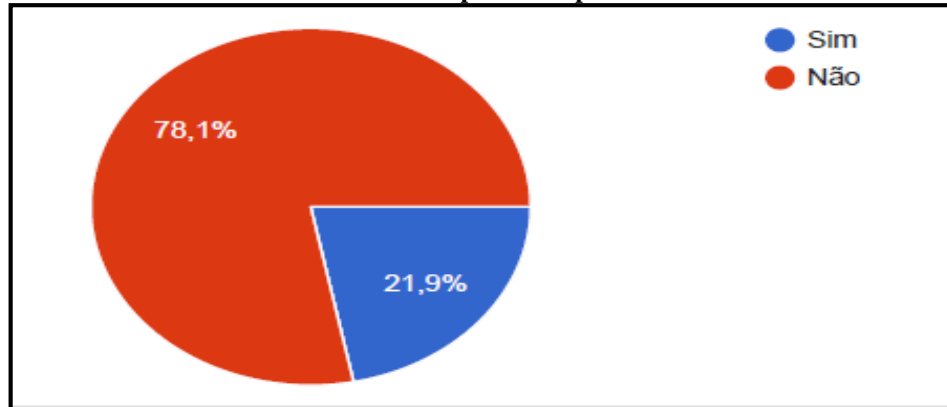
Gráfico 04 – Conhecimentos temáticos importantes para combate a crimes cibernéticos



Fonte: Elaborado pelo autor (2023)

A importância dos conhecimentos acima citados, levou a questionar sobre a formação do entrevistado. E a pesquisa apontou um número elevado de participantes que afirmaram não ter uma disciplina que trabalhe esses conhecimentos, como mostrado no gráfico abaixo:

Gráfico 05 – Conhecimentos temáticos importantes para combate a crimes cibernéticos

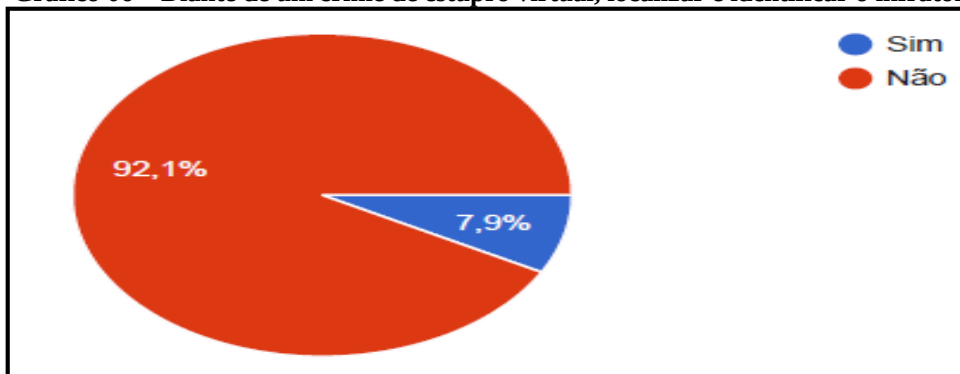


Fonte: Elaborado pelo autor (2023)

Os dados também demonstraram que o policial militar não está preparado para

investigar um crime virtual, conforme apresentado no Gráfico 06, onde foram questionados se diante de uma denúncia de estupro virtual, saberiam como buscar a localização virtual e identificar o infrator, e dos 64 questionários, 92,1% responderam que não saberiam. Ressaltando que dos 64 respondentes 01 questionado não respondeu a essa questão.

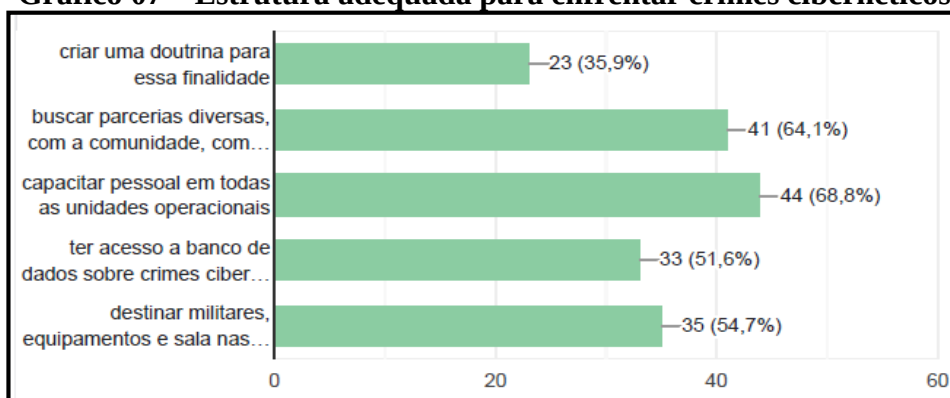
Gráfico 06 – Diante de um crime de estupro virtual, localizar e identificar o infrator



Fonte: Elaborado pelo autor (2023)

A pergunta 07, inquiriu o pesquisado sobre a estrutura adequada para lidar com crimes cibernéticos pela Polícia Militar Ostensiva, e na opinião dos entrevistados o que é necessário para executar esse trabalho. Essa questão foi aberta para mais de uma resposta. Das quais, 44 afirmam que a capacitação pessoal em todas as unidades operacionais, é o quesito mais importante; 41 respostas apontaram a importância de parcerias com a comunidade, o Poder Judiciário e outras instituições; 35 afirmaram ser necessário destinar militares, equipamentos e sala nas unidades, para lidarem exclusivamente com os crimes cibernéticos. Enfim, os resultados apontaram que a Polícia Militar Ostensiva, ainda não está preparada para combater efetivamente os crimes virtuais.

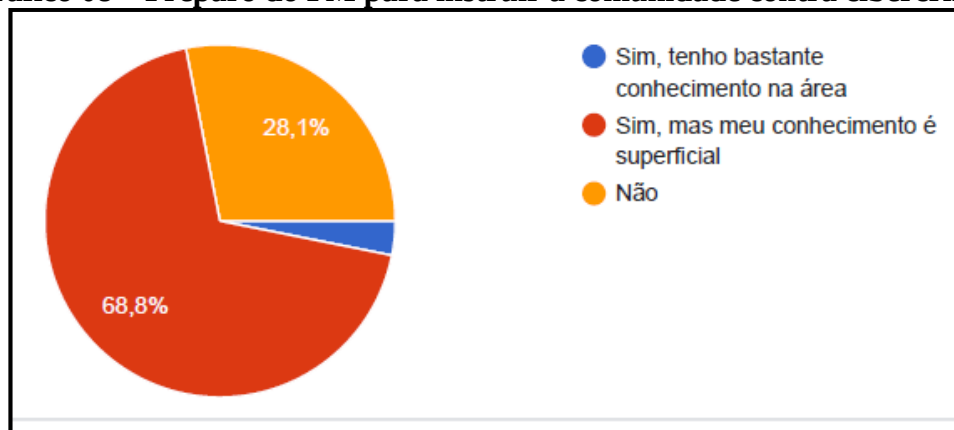
Gráfico 07 – Estrutura adequada para enfrentar crimes cibernéticos



Fonte: Elaborado pelo autor (2023)

Por fim a pesquisa questionou os entrevistados se este se sente preparado para instruir a comunidade a se precaver contra os golpes praticados via internet, apresentando inclusive formas de proteção de dados para o cidadão. E nesta questão 68,8% responderam que sim, mas que seu conhecimento é superficial, 28,1% disseram que não, e apenas uma parcela bem pequena disse ter bastante conhecimento na área para atender a comunidade. Veja Gráfico 08:

Gráfico 08 – Preparo do PM para instruir a comunidade contra ciber Crimes



Fonte: Elaborado pelo autor (2023)

Os dados acima, demonstram o despreparo dos policiais militares sobre o tema abordado. Hoje, as ferramentas tecnológicas facilitam na aquisição da aprendizagem em qualquer área, de forma que é necessário levar aos agentes de segurança pública, os conhecimentos necessários em todas as áreas de atuação. Assim como os criminosos se aperfeiçoam na prática de atos ilícitos através dessas ferramentas o agente também precisa estar preparado.

4 CONSIDERAÇÕES FINAIS

Diante dos resultados da pesquisa, percebe-se que a Polícia Militar de Goiás não está preparada para atuar nessa área. Os conhecimentos apontados como ideais para combater esse tipo de crime, não constam nas disciplinas da Matriz Curricular apresentada no Quadro 01, assim como os ciclos 1, 2 e 3/2023 que possui cursos diversos, porém não constam disciplinas que aplique conhecimentos específicos sobre a temática que envolve a investigação de ciber crimes.

Outros cursos como os ofertados pela Gestão e Ensino em Segurança Pública (SEGEN), como cursos à distância, tratam de forma mais detalhada e específica, porém não foi observada nenhuma obrigatoriedade dos policiais militares em cursá-los. Pereira (2013) afirma que há

cursos direcionados a oficiais, praças, ou aos dois, e que é função da Superintendência da Academia Estadual de Segurança Pública coordenar o ensino de acordo com as diretrizes.

A ampliação dos conhecimentos teóricos e práticos aperfeiçoa as qualidades e aptidões em todas as áreas do conhecimento melhorando a qualidade na execução de qualquer tarefa profissional. Nesse contexto, esta pesquisa conseguiu atingir seus objetivos, demonstrando que os cursos oferecidos não abarcam conhecimentos sobre a temática, mostrando o despreparo do agente policial em atuar no auxílio às polícias investigativas, assim como ocorre em outros estados brasileiros. Também faltam materiais e equipamentos para treinamento e execução das tarefas necessárias à investigação criminal.

Sendo assim, é importante ressaltar a necessidade de ampliar o leque de discussões sobre os aspectos que envolvem os crimes cibernéticos, na busca de práticas inovadoras que venham punir efetivamente os criminosos que utilizam o ambiente virtual.

5 REFERÊNCIAS

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada**. 2021. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contr-crimes-ciberneticos-e-sancionada>>. Acesso em: 20 ago. 2023

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Brasília: Casa Civil, 2021. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 03 set. 2023.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Brasília: Casa Civil, 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 03 set. 2023.

_____. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Brasília: Casa Civil, 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 03 set. 2023.

CARNEIRO, Leonardo de. **Ferramentas digitais para aprendizagem colaborativa nos cursos de qualificação profissional da Polícia Militar do Tocantins**. 2019. Dissertação (Mestrado em Modelagem Computacional de Sistemas) Universidade Federal do Tocantins. Palmas, TO: UFTO, 2019. Disponível em: <<https://repositorio.uft.edu.br/bitstream/11612/1597/1/Leonardo%20de%20Andrade%20Carneiro%20-%20Disserta%C3%A7%C3%A3o.pdf>>. Acesso em: 03 set. 2023.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. 2006. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro. Rio de Janeiro: UFRJ, 2006. Disponível em: <<https://www.cos.ufrj.br/uploadfile/1430748034.pdf>>. Acesso em: 10 set. 2023.

CORREA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet**. 2013. Dissertação (Mestrado em Ciências) – Faculdade de Filosofia, Ciências e Letras da Universidade de São Paulo. Ribeirão Preto, SP: FFCLRP; USP, 2013. Disponível em: <<https://teses.usp.br/teses/disponiveis/59/59137/tde-08102013-162610/es.php>>. Acesso em: 20 ago. 2023.

CORREA, Mauro Luciano. **A formação do policial militar dentro e fora dos portões da instituição**. 2018. Disponível em: <<https://acervodigital.ssp.go.gov.br/pmgo/handle/123456789/1861>>. Acesso em: 20 ago. 2023.

COSTA, Emanuely Silva; SILVA, Raíla da Cunha, Crimes cibernéticos e investigação policial. **Rev. Eletrônica do Ministério Público do Estado do Piauí**, ed. 02, ano 01, 2021. Disponível em: <<https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf>>. Acesso em: 22 ago. 2023.

DALBERIO, Osvaldo.; DALBERIO, Maria Célia Borges. **Metodologia científica: desafios e caminhos**. São Paulo: Paulus, 2009.

FERNANDES, Fagner. **Inteligência cibernética: produção de conhecimento com segurança**. SENASP, 2023. Disponível em: <http://portal.ead.senasp.gov.br/academico/copy2_of_editoria-a/introducao-a-atividade-de-inteligencia>. Acesso em: 27 set. 2023.

FERNANDES, Fagner. **Deteção de fraudes eletrônicas em períodos de crise**. SENASP, 2023. Disponível em: <http://portal.ead.senasp.gov.br/academico/copy_of_editoria-a/deteccao-de-fraudes-eletronicas-em-periodos-de-crise>. Acesso em: 27 set. 2023.

FERNANDES, Fagner. **Crimes cibernéticos: noções básicas**. SENASP, 2023. Disponível em: <http://portal.ead.senasp.gov.br/academico/copy_of_editoria-a/crimes-ciberneticos-noco-es-basicas>. Acesso em: 27 set. 2023

FERNANDES, Fagner. **PAEP 2021**. SENASP, 2021. Disponível em: <http://portal.ead.senasp.gov.br/academico/copy_of_editoria-a/portfolio-2021>. Acesso em: 27 set. 2023.

FERREIRA, Rafaela. **Aumento do uso da internet faz crescer o número de crimes cibernéticos.** 2022. Disponível em: <<https://www.jornalopcao.com.br/ultimas-noticias/aumento-do-uso-da-internet-faz-crescer-o-numero-de-crimes-ciberneticos-374687/>>. Acesso em: 23 ago. 2023.

FERREIRA, Sarah Pereira. **Crimes cibernéticos: a ineficácia da legislação brasileira.** 2021. Artigo Científico (DIREITO) - Pontifícia Universidade Católica de Goiás. Goiânia: PUCGOIÁS, 2021. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1709/1/Artigo%20Cientif%C3%ADco-%20Sarah%20Pereira%20Ferreira.pdf>>. Acesso em: 20 ago. 2023.

FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** 2019. Disponível em: <<https://jus.com.br/imprimir/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos>>. Acesso em: 21 ago. 2023.

MARTINS, Alexander Dias. **A atuação da polícia militar de Minas Gerais na prevenção e repressão aos crimes cibernéticos.** 2010. Monografia (Especialização em Segurança Pública) – Academia de Polícia Militar de Minas Gerais; Fundação João Pinheiro. Belo Horizonte, MG, 2010. Disponível em: <<http://monografias.fjp.mg.gov.br/handle/123456789/1764>>. Acesso em: 22 ago. 2023.

MINAYO, Maria Cecília de Souza (org.). **Pesquisa social: Teoria, método e criatividade** 18. ed. Petrópolis: Vozes, 2001.

MITNICK, Kevin D. **A arte de enganar.** Tradução de Kátia Aparecida Roque. São Paulo: Pearson Education, 2003. Disponível em: <https://www.academia.edu/7428475/A_arte_de_enganar_kevin_mitnick>. Acesso em: 08 out. 2023.

PENHA, Marcelo; PENHA, Renato; ANDRADE, Diego César Terra de. Inovação em serviços de comunicação: utilização de mídias sociais pela Polícia Militar para redução do índice criminal. **REBESP**, Goiânia, n. 1, v. 13, p. 01-08, 2020. Disponível em: <<https://revista.ssp.go.gov.br/index.php/rebsp/article/view/398>>. Acesso em: 20 ago. 2023.

PEREIRA, Elio Gomes. **O ensino na academia da polícia militar em Goiás: matrizes curriculares – mudanças e permanências 1970-2012.** 2013. Dissertação (Mestrado em História Cultura e Poder) – Pontifícia Universidade Católica de Goiás. Goiânia: PUCGO, 2013. Disponível em: <<https://tede2.pucgoias.edu.br/bitstream/tede/3312/1/ELIO%20GOMES%20PEREIRA.pdf>>. Acesso em: 27 set. 2023.

QUEIROZ, Gabriel Ferreira. **Cibercriminalidade no Brasil: aplicação, falibilidade e impunidade**. 2021. Artigo Científico (DIREITO) - Pontifícia Universidade Católica de Goiás. Goiânia: PUCGOIÁS, 2021. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2960/1/TCC-%20GABRIEL%20FERREIRA%20QUEIROZ%20%20.pdf>>. Acesso em: 20 ago. 2023.

SENASP. **Matriz curricular nacional para ações formativas dos profissionais da área de segurança pública**. Brasília: SENASP, 2014. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/gestao-e-ensino/site-novo/matrizcurricularnacional_versaofinal_2014.pdf>. Acesso em: 03 set. 2023.

SOUZA, Baltazar Donizete de. **O ensino policial e a formação de oficiais na academia de polícia militar do estado de Goiás**. 2003. Dissertação (Mestrado em Educação). Universidade Católica de Goiás. Goiânia: UCG, 2003. Disponível em: <<https://tede2.pucgoias.edu.br/bitstream/tede/3779/2/BALTAZAR%20DONIZETE%20DE%20SOUZA.pdf>>. Acesso em: 20 ago. 2013.

SOUZA, Mayara Castro de. **Da necessidade da presença à ausência: formação da polícia militar no Distrito Federal, direitos humanos e questão racial**. 2020. Dissertação (Mestrado em Direitos Humanos e Cidadania) – Universidade de Brasília. Brasília: UNB, 2020. Disponível em: <<https://repositorio.unb.br/handle/10482/40521>>. Acesso em: 20 ago. 2023.

APÊNDICE A - QUESTIONÁRIO

Esse formulário com oito questões tem como finalidade comprovar ou refutar as questões levantadas na pesquisa sobre o **Combate ao cibercrime: aspectos da formação e preparo do policial militar no Estado de Goiás**, que estou desenvolvendo, como requisito para minha especialização no curso de Pós-Graduação em Segurança Pública. Conto com sua gentileza de responder as questões abaixo, para que a pesquisa seja entregue dentro do prazo exigido no curso. Suas respostas contribuirão para a pesquisa, que pretende apresentar medidas para implementação da atuação do profissional militar no combate a essa prática que vem crescendo no Estado. Não é necessário se identificar.

1) Você já desconfiou de um golpe devido a uma das situações abaixo, em que a pessoa do outro lado da linha telefônica:

- a) ☐ Se recusou a dar um número de retorno
- b) ☐ Afirmou que o não atendimento imediato acarretaria em algum tipo de perda, por exemplo financeira
- c) ☐ Alegou ser uma autoridade e deu ênfase na urgência de concluir a solicitação
- d) ☐ Fez uma solicitação fora do comum

2) Se você sofresse um golpe cibernético, como você agiria?

- a) ☐ Tenho conhecimento suficiente para tomar as medidas cabíveis
- b) ☐ Buscaria ajuda de especialistas na PMGO
- c) ☐ Buscaria ajuda de especialistas na PCGO

3) Você tem conhecimento sobre crimes cibernéticos?

- a) ☐ sim, conheço amplamente
- b) ☐ sim, porém tenho pouco conhecimento
- c) ☐ não tenho conhecimento

4) Indique quais desses temas faz parte dos seus conhecimentos **(pode marcar mais de uma opção)**

- a) ☐ Algoritmo e Programação estruturada
- b) ☐ Criptografia
- c) ☐ Lógica computacional
- d) ☐ Linguagem de programação
- e) ☐ Programação para redes
- f) ☐ Privacidade e proteção de dados

5) Em sua formação no curso de especialização em Segurança Pública, houve alguma disciplina

que tratasse os conhecimentos apresentados na questão 04?

- a) ☐ Sim
- b) ☐ Não
- c) ☐ Alguns. Quais? _____

6) Diante de uma denúncia de prática de crime de estupro virtual, você saberia como buscar a localização virtual e identificar o infrator?

- a) ☐ Sim
- b) ☐ Não

7) Na sua opinião, para que a Polícia Militar Ostensiva seja adequadamente estruturada, a fim de lidar com os crimes cibernéticos, ela precisa: (pode marcar mais de uma opção)

- a) ☐ criar uma doutrina para essa finalidade
- b) ☐ buscar parcerias diversas, com a comunidade, com o Poder Judiciário, com as demais forças policiais (estaduais e federais) e com entidades que lidam com a questão
- c) ☐ capacitar pessoal em todas as unidades operacionais
- d) ☐ ter acesso a banco de dados sobre crimes cibernéticos
- e) ☐ destinar militares, equipamentos e sala nas unidades, para lidarem exclusivamente com os crimes cibernéticos.

8) Você se sente preparado para instruir a comunidade a se precaverem contra golpes praticados pela internet, apresentando inclusive formas de proteção de dados?

- a) ☐ Sim, tenho bastante conhecimento na área
- b) ☐ Sim, mas meu conhecimento é superficial
- c) ☐ Não