Cibercrime em Mato Grosso: Uma Análise Quantitativa da Evolução dos Ataques

Felipe Fonteles Belo[1], Nelcileno Virgilio de Souza Araújo[1], Constantino Dias da Cruz Neto[2]

[1] Instituto de Computação - Universidade Federal de Mato Grosso – Av. Fernando Corrêa da Costa, nº 2367 Bairro Boa Esperança - CEP: 78060-900 - Cuiabá - MT

[2]Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso – Campus Cuiabá Cel. Octayde Jorge da Silva - Rua Profa. Zulmira Canavarros, 95 - CEP: 78005-200 - Cuiabá - MT - Brasil

{felipebelo@live.com, nelcileno.araujo@ufmt.br, constantino.neto@ifmt.edu.br}

Abstract. *Cybercrime is a growing threat in Mato Grosso, demanding attention and effective countermeasures.This study aims to analyze the evolution of cybercrime in the state between 2019 and 2023, seeking to understand attack patterns, strategies, and vulnerabilities.Through a quantitative approach, data from police reports will be examined, identifying the most frequent types of digital crimes and main trends. The results reveal a significant increase in the incidence of cybercrimes in Mato Grosso during the period analyzed, with emphasis on fraud and online fraud. The study demonstrates the effectiveness of quantitative analysis of police reports to understand the evolution of cybercrime in the state.*

Resumo. *O cibercrime representa uma ameaça crescente em Mato Grosso, demandando atenção e medidas eficazes de combate. Este estudo tem como propósito analisar a evolução do cibercrime no estado entre 2019 e 2023, buscando compreender os padrões de ataque, estratégias e vulnerabilidades. A partir de uma abordagem quantitativa, serão examinados dados de boletins de ocorrência, identificando os tipos de crimes digitais mais frequentes e as principais tendências. Os resultados revelam um aumento significativo na incidência de cibercrimes em Mato Grosso no período analisado, com destaque para estelionato e fraudes online. O estudo demonstra a efetividade da análise quantitativa de boletins de ocorrência para a compreensão da evolução do cibercrime no Estado.*

1. Introdução

A era digital trouxe consigo uma série de facilidades e comodidades, mas também abriu portas para um novo tipo de criminalidade: o cibercrime [Furnell 2010]. A popularização da internet e dos dispositivos conectados, tais como: *smartphones* e computadores criou um terreno fértil para criminosos explorarem vulnerabilidades e aplicarem golpes virtuais. Redes sociais, lojas online e aplicativos de mensagens instantâneas, apesar de úteis, tornaram-se ferramentas para a disseminação de ameaças como *phishing*, *ransomware* e engenharia social [Walters 2023].

O cibercrime tem se tornado uma realidade cada vez mais presente no cotidiano da sociedade, impactando indivíduos, empresas e governos em diversas partes do mundo, segundo o [CERT.br 2023], o número de incidentes de segurança cibernética reportados no Brasil aumentou significativamente nos últimos anos, o que corrobora a afirmação de que o país, incluindo o estado de Mato Grosso, tem enfrentado um desafio crescente em relação aos crimes digitais e necessita de medidas eficazes para combatê-los.

Este artigo se dedica a analisar a evolução do cibercrime em Mato Grosso entre os anos de 2019 e 2023, a partir de uma perspectiva quantitativa. A pesquisa se baseia na análise de dados extraídos de boletins de ocorrência registrados nesse período, buscando identificar padrões, tendências e mudanças no *modus operandi* dos cibercriminosos.

O artigo está estruturado em seções que exploram aspectos importantes do cibercrime. Inicialmente, será apresentada uma contextualização sobre o tema. Em seguida, na seção Metodologia, serão descritos os procedimentos metodológicos utilizados para definir o comportamento do cibercrime em Mato Grosso, com foco na análise dos boletins de ocorrência registrados nos últimos 5 anos. A seção de Resultados e Discussões, apresenta a análise de dados dos boletins de ocorrências, considerando os padrões de sazonalidade, tipo de crime digital e temporalidade. Por fim, a seção Conclusão responde aos objetivos da pesquisa, apresentando as conclusões sobre a evolução do cibercrime em Mato Grosso e as implicações para a sociedade mato-grossense, com sugestões de medidas preventivas e de combate ao cibercrime.

2. Cibercrime e sua Tipificação

O cibercrime, também conhecido como crime digital, crime informático ou crime virtual, é definido como qualquer ato ilícito que utilize a tecnologia da informação e comunicação (TIC) como meio ou alvo para sua prática [Lima 2021]. É destacado por [Ramos e Santos 2022] a importância de se reconhecer a fragilidade do ordenamento jurídico em relação à tipificação e punição desses crimes, que se escondem por trás da tela do computador, deixando vítimas expostas em suas vidas reais.

É fundamental diferenciar os crimes cibernéticos próprios, que têm como alvo sistemas informáticos, tais como: a invasão de dispositivos, e crimes cibernéticos impróprios, que utilizam o sistema informático como meio para cometer crimes tradicionais, tais como: o estelionato e a difamação [Lima 2021]. A crescente variedade de cibercrimes exige uma categorização para melhor compreensão e desenvolvimento de estratégias eficazes de combate [Al-Khater et al. 2020]. No Quadro 1 descreve-se, conforme literatura analisada, a tipificação do cibercrime [Syafitri et al. 2022] [Al-Khater et al. 2020] [Aslan 2023] [Kaspersky 2023].

O cibercrime, assim como o crime tradicional, pode ser descrito pelo chamado triângulo do crime [Cross & Shinder 2008], que estabelece que três fatores precisam estar presentes para que um crime ocorra: uma vítima, um motivo e uma oportunidade. A vítima é o alvo do ataque, a motivação seria o que leva o criminoso a cometer o ataque, e a oportunidade a condição que permite que o crime ocorra (por exemplo, uma vulnerabilidade no sistema ou um dispositivo sem proteção).

Quadro 1. Tipificação do cibercrime.

Tipos de Cibercrime		Descrição
Crimes contra a pessoa	Assédio cibernético	Inclui o *cyberbullying, stalking* e outras formas de perseguição online.
	Pornografia infantil	Envolve a produção, distribuição e posse de material que explore sexualmente crianças e adolescentes.
	Crimes contra a honra	Abrangem a difamação, calúnia e injuria online.
	Furto de identidade	Ocorre quando criminosos roubam informações pessoais para fins fraudulentos.
Crimes contra o patrimônio	Fraudes financeiras	Incluem o *phishing*, golpes em e-commerce, clonagem de cartões e transferências bancárias fraudulentas.
	Ransomware	Ataques que criptografam dados e exigem pagamento de resgate para sua liberação
	Extorsão	Chantagem online com base em informações confidenciais ou material comprometedor da vítima.
Crimes contra a segurança da informação	Invasão de dispositivos	Acesso não autorizado a computadores, smartphones e outros dispositivos.
	Ataques de negação de serviço	Visam sobrecarregar servidores e sistemas
	Disseminação de malware	Propagação de vírus, *worms, spywares* e outros softwares maliciosos
Outros tipos de cibercrime	Crimes de ódio	Disseminação de mensagens de ódio e preconceito online.
	Desinformação	Propagação de notícias falsas e informações enganosas.
	Ciberterrorismo	Utilização da internet para fins terroristas.

3. Metodologia

A metodologia do projeto envolve etapas definas e estruturadas. Algumas etapas são desenvolvidas em paralelo, enquanto outras dependem dos subsídios fornecidos pela conclusão da etapa anterior para a execução da próxima. A pesquisa proposta se estrutura em uma metodologia quantitativa e em partes qualitativa, com foco na análise dos boletins de ocorrência registrados em Mato Grosso nos últimos 5 anos, será utilizado ferramentas de IA e criação de gráficos como *Gemini* e *GraphMaker* como apoio para tratamento dos dados. Nesta pesquisa iremos buscar, em cada período, identificar padrões nos tipos de

crimes, nas formas de ataque, nos alvos preferenciais dos criminosos e nas estratégias utilizadas de acordo com os Boletins de Ocorrência 2019-2023.

A análise dos dados coletados se dará por meio da compreensão de padrões, traçando a evolução do cibercrime ao longo do período, avaliando se existiram mudanças significativas em determinados meses do ano, ou durante os anos analisados, também nos tipos de crimes e se as estratégias dos criminosos se tornaram mais sofisticadas, com a investigação dos métodos e ferramentas de ataque, além de observar as principais tendências e o perfil das vítimas. Os resultados obtidos serão analisados para corroborar com as informações da literatura existente e artigos semelhantes, para que assim possa ser encontrado uma melhor compreensão do tema da pesquisa.

4. Resultado e Discussões

Para desenvolver as devidas análises e formular ideias e conclusões, seria necessário obter dados concisos e fidedignos, então foi realizado o pedido formal ao Gabinete da Secretaria Adjunta de Inteligência - GAB/SAI/SESP do Estado de Mato Grosso, para que assim possamos obter acesso ao máximo de informação a respeito dos boletins de ocorrência do estado entre 2019 a 2023, a secretaria nos forneceu dados de forma bruta através de uma planilha na extensão CSV, esta planilha estava estruturada com a quantidade de BOs por natureza da ocorrência, municípios, ano e mês.

Inicialmente, a planilha de dados foi organizada e refinada no Excel, com a remoção de entradas duplicadas, correção de erros de digitação e formatação adequada para análise. Essa etapa de ajuste manual foi crucial para garantir a confiabilidade dos dados, posteriormente, as ferramentas *Gemini* e *GraphMaker* foram utilizadas para a criação dos gráficos.

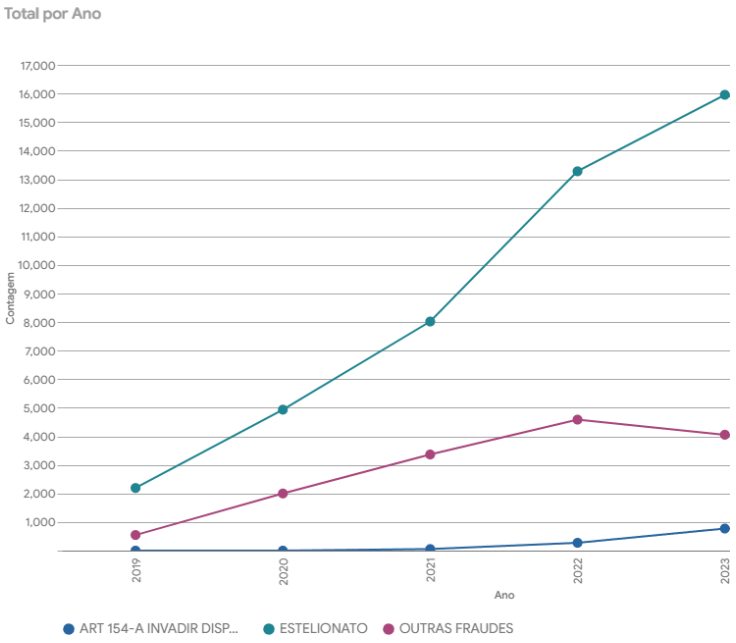

Figura 1 - Evolução anual do total de boletins de ocorrência (BOs) por tipo de crime, de 2019 a 2023.

Na Figura 1, observa-se um aumento significativo nos registros de estelionato a partir de 2020, coincidindo com o início da pandemia de COVID-19, que de acordo com o [Fórum Brasileiro De Segurança Pública 2024], o período pandêmico foi marcado pela intensificação das atividades online, o que ampliou as oportunidades para a aplicação de golpes virtuais, o isolamento social e as medidas de restrição impostas durante a pandemia levaram a um aumento significativo do uso de serviços bancários digitais e compras online, o que aumentou a exposição das pessoas a ataques cibernéticos, como *phishing* e fraudes em compras online.

Além disso, também é mencionado pelo Anuário Brasileiro de Segurança Pública de 2024 que a pandemia acelerou a transformação digital, com a migração de diversas atividades para o ambiente virtual. O trabalho remoto, a educação a distância e o aumento do uso de redes sociais e aplicativos de mensagens instantâneas tornaram a população mais vulnerável a golpes virtuais, especialmente aqueles que exploram a vulnerabilidade humana, tais como o estelionato. Estes dados informados pelo Anuário indicam que o estelionato digital se tornou uma das principais ameaças à segurança pública durante a pandemia, explorando a vulnerabilidade das pessoas em um momento de incertezas e dificuldades [Fórum Brasileiro De Segurança Pública 2024].

O crime de invasão de dispositivo informático, representado pela linha azul escuro, não apresentou o mesmo crescimento que o estelionato durante a pandemia da COVID-19. Esse comportamento pode ser explicado pela natureza e pela forma de execução desses crimes. De acordo com [Jornal da USP 2023], o número de registros de invasão de dispositivo informático se manteve relativamente estável durante a pandemia, apresentando apenas uma leve tendência de aumento, o que corrobora o gráfico supracitado.

O terceiro tipo representado pela linha rosa, com o nome “outras fraudes”, seria uma categoria que pode englobar diferentes tipos de fraudes online, porém pelas informações fornecidas pela SESP, não é possível especificar as tipificações de cibercrimes para essa classe. Observa-se um aumento significativo desta entre 2019 e 2022, seguido de uma leve queda em 2023, apesar da queda, os números ainda são altos, evidenciando a necessidade de atenção e medidas de prevenção. É observado que esta categoria tem uma ocorrência maior que invasão de dispositivos e menor do que estelionato, indicando assim, que esta classe, pode conter diversos tipos de crimes digitais não catalogados dentro de uma só classificação, demonstrando a falta de mais detalhes nos relatórios da SESP, contudo, há uma dificuldade grande de se observar estes dados em esfera nacional, de acordo com o Anuário Brasileiro de Segurança Pública de 2024, muitos estados não contabilizam de forma separada do total estes tipos de crimes.

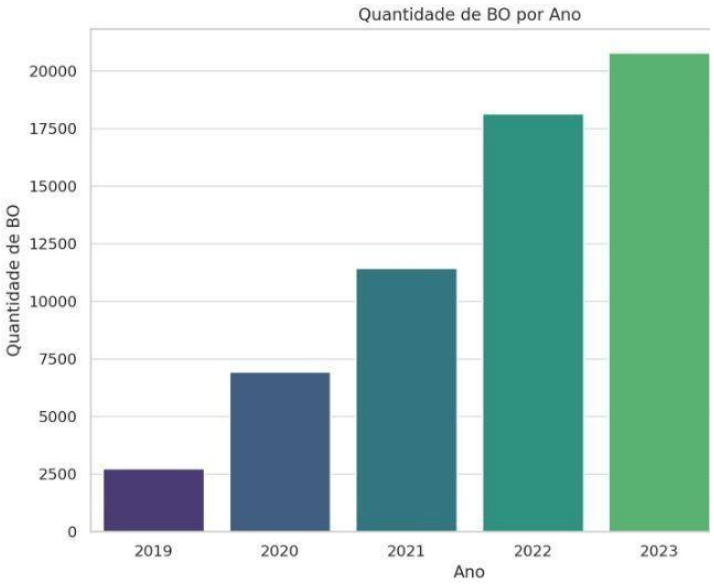

Figura 2 - Evolução do total de boletins de ocorrência BOs, registrados anualmente de 2019 a 2023.

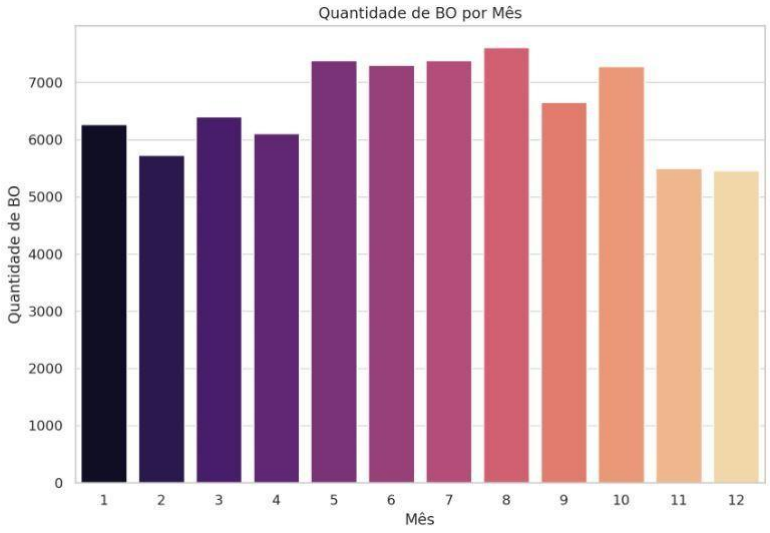

Figura 3 – Média de quantidade por mês nos anos de 2019 a 2023.

Observa-se na Figura 2 um aumento significativo na quantidade de boletins de ocorrência relacionados a crimes cibernéticos entre 2019 e 2023. O ano de 2023 apresentou o maior número de registros, demonstrando o crescimento dos crimes digitais no estado, que anteriormente não eram catalogados. A Figura 3 demonstra uma sazonalidade nos registros de crimes cibernéticos, com picos nos meses de maio, junho, julho e agosto, essa sazonalidade pode estar relacionada a fatores, tais como: férias escolares, datas comemorativas e períodos de maior movimentação financeira, tal como o pagamento de décimo terceiro salário, o que já foi observado nas literaturas mencionadas e no artigo de Lallie et al. (2021).

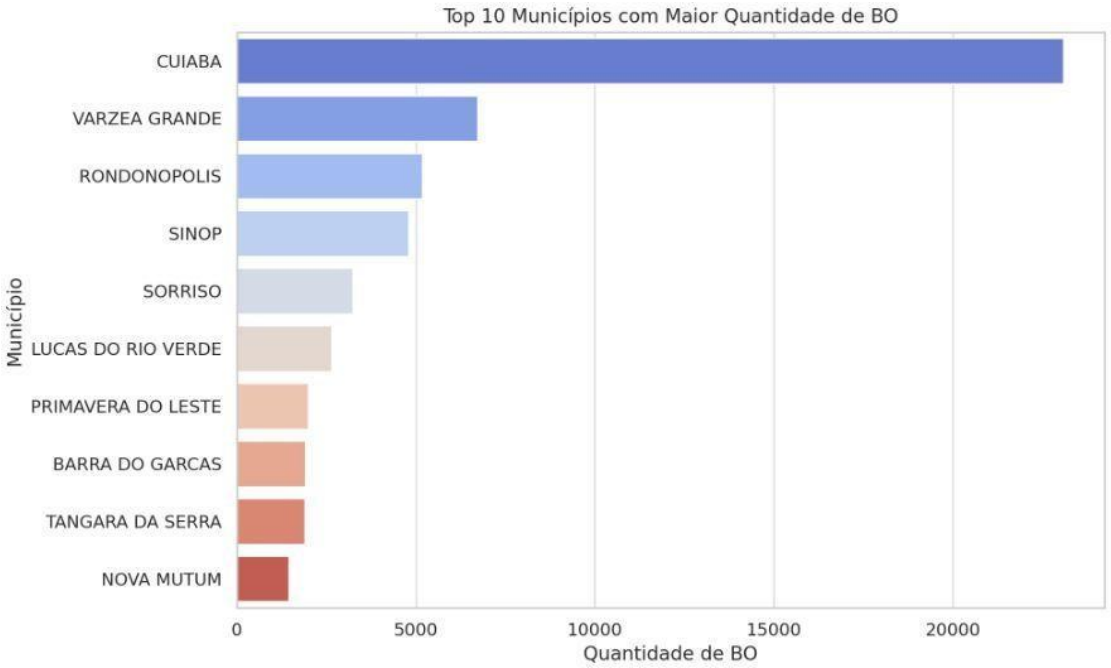

Figura 4 – Quantidade de BOs nos principais municípios, de 2019 a 2023.

A Figura 4 apresenta a distribuição dos boletins de ocorrência (BOs) relacionados a crimes cibernéticos nos principais municípios de Mato Grosso entre 2019 e 2023, evidenciando a concentração desses crimes em áreas urbanas mais populosas, como Cuiabá, Várzea Grande e Rondonópolis. Essa análise complementa os dados das Figuras 1, 2 e 3, que destacam o crescimento exponencial de crimes como estelionato e fraudes online, além de padrões sazonais observados ao longo do período. A literatura utilizada no artigo, como os estudos de Lallie et al. (2021) e Kumar et al. (2022), destaca que a digitalização acelerada durante a pandemia de COVID-19 não apenas ampliou a dependência de tecnologias digitais, mas também expôs a população a novas vulnerabilidades, criando um ambiente propício para o aumento dos cibercrimes.

Os gráficos demonstram que o cibercrime em Mato Grosso está em ascensão, com destaque para o estelionato e outras fraudes online. Apesar de uma relativa estabilidade na incidência do crime de invasão de dispositivo informático na Figura 1, é necessário aprofundar a análise, explorando dados concretos e literatura relevante, para investigar se esse fenômeno pode estar relacionado a fatores como a maior eficácia das medidas de segurança contra esse tipo de ataque ou o redirecionamento dos criminosos para modalidades de crimes mais rentáveis. Somente com esse aprofundamento será possível sustentar conclusões mais robustas e fundamentadas.

Conforme apontado por [Lima & Viana 2022], o aumento do cibercrime é impulsionado por uma combinação de fatores socioeconômicos e tecnológicos. O acesso ampliado à internet e a popularização de dispositivos conectados criam um ambiente favorável à atuação de criminosos. Dados da pesquisa realizada pela [Revista Forense Digital 2023] indicam que a digitalização de serviços bancários e comerciais aumentou significativamente as oportunidades para fraudes eletrônicas. No contexto específico do estelionato, o crescimento exponencial observado (oito vezes nos últimos cinco anos, conforme Figura 2) pode estar atrelado à falta de conscientização dos usuários que continuam sendo alvos fáceis de golpes devido à carência de educação digital [Lima &

Viana 2022], Estudos do [Jornal da USP 2023] ressaltam que as técnicas de engenharia social utilizadas pelos criminosos se tornam cada vez mais sofisticadas, dificultando a identificação de fraudes, além disso, a legislação brasileira ainda enfrenta desafios para lidar com a dinâmica do cibercrime, como apontado por [Revista Forense Digital 2023]. A falta de regulamentações atualizadas e de recursos especializados nas forças policiais contribui para a impunidade e, consequentemente, para a perpetuação desses crimes.

Com base na análise dos gráficos e nas informações extraídas dos artigos, torna-se claro a necessidade de ações conjuntas entre o Estado, a Secretaria de Segurança Pública e a sociedade para combater o cibercrime em Mato Grosso. A criação de políticas públicas eficazes, com foco em prevenção, conscientização e educação digital, pode ser fundamental para reduzir a vulnerabilidade da população e promover um ambiente digital mais seguro.

O aumento dos cibercrimes em Mato Grosso durante e após a pandemia de COVID-19 reflete uma tendência global que foi observada no estudo de Kumar et al. (2022) no qual é descrito que a pandemia como uma "pandemia cibernética silenciosa", destacando que o isolamento social e a dependência de tecnologias digitais criaram um ambiente propício para ataques como *phishing* e *ransomware.* Esses ataques exploraram a ansiedade e a desinformação da população, utilizando temas relacionados tanto a COVID-19 quanto outros eventos de cunho público, assim como Lallie et al. (2021) menciona que criminosos cibernéticos sempre buscam maximizar seus ganhos e, por isso, esperam pelo momento certo para lançar ataques. Desastres naturais, crises em andamento ou eventos públicos de grande repercussão criam condições ideais para esse tipo de ataque. No contexto de Mato Grosso, o crescimento exponencial de estelionatos digitais e fraudes online, conforme demonstrado pelos boletins de ocorrência analisados, está alinhado com essa dinâmica global, evidenciando a vulnerabilidade da população em momentos de crise [Lallie et al. 2021].

A análise cronológica de Lallie et al. (2021) reforça a conexão entre eventos específicos, tais como: anúncios governamentais e programas de auxílio financeiro, e o aumento de ataques cibernéticos. No Reino Unido, por exemplo, campanhas de *phishing* foram moldadas para explorar anúncios de *lockdown* e benefícios sociais logo após anúncios oficiais do governo na mídia, o que também pode ser observado em Mato Grosso, onde picos de crimes digitais coincidiram com períodos de maior movimentação financeira, como o pagamento do auxílio emergencial. Essa relação entre eventos e ataques destaca a importância de estratégias preventivas que antecipem os movimentos dos cibercriminosos, especialmente em momentos de maior vulnerabilidade social.

Além disso, Kumar et al. (2022) sugerem que contramedidas proativas, tais como o uso de inteligência artificial e a educação em segurança digital, são essenciais para mitigar os impactos dos cibercrimes. No caso de Mato Grosso, a categorização detalhada dos crimes digitais, como estelionato e fraudes financeiras, é fundamental para o desenvolvimento de políticas públicas direcionadas. A falta de conscientização da população sobre práticas seguras no ambiente digital, apontada tanto neste estudo quanto nos artigos internacionais, reforça a necessidade de maior investimento em campanhas educativas para conscientização da sociedade.

A Secretaria de Segurança Pública pode atuar na capacitação de mais policiais para a investigação e combate ao cibercrime, além de investir em ferramentas e tecnologias para a coleta e análise de evidências digitais. A criação de um formulário mais

completo para registro de boletins de ocorrência, com informações específicas sobre o tipo de crime, método utilizado e plataforma digital envolvida, permitirá uma melhor tipificação dos crimes digitais e contribuirá para a produção de estatísticas mais precisas, subsidiando a tomada de decisão e a formulação de políticas públicas direcionadas. A colaboração entre o Estado a Secretaria de Segurança Pública e a sociedade civil, com a participação de universidades, empresas e organizações não governamentais, é fundamental para o desenvolvimento de estratégias eficazes de combate ao cibercrime em Mato Grosso.

5. Conclusão

Conclui-se que o cibercrime em Mato Grosso, assim como no Brasil e no mundo, é um problema crescente e dinâmico, demandando atenção e medidas eficazes de combate. A análise dos boletins de ocorrência e dos artigos científicos estudados evidenciou um aumento preocupante nos casos de cibercrimes, especialmente estelionato e fraudes online, o que exige atenção e medidas eficazes de prevenção e combate.

A concentração de ocorrências na capital e nas maiores cidades do estado, sugere a necessidade de ações direcionadas a essas regiões, considerando o perfil socioeconômico da população e o acesso à internet. A sazonalidade observada em alguns tipos de crimes indica a importância de intensificar as medidas de segurança em períodos específicos, como datas comemorativas, crises e eventos públicos de grande repercussão, quando a vulnerabilidade a golpes pode ser maior. É crucial que a população sempre esteja informada sobre os riscos do cibercrime e saiba como se proteger, identificando mensagens fraudulentas e adotando práticas seguras no uso da internet. A educação e a conscientização são ferramentas essenciais no combate ao cibercrime, em conjunto com políticas públicas eficazes e o desenvolvimento de soluções de segurança.

Referências

Furnell, S. (2010) “Cybercrime: Vandalizing the Information Society”, Boston: Addison-Wesley.

Walters, R. (2023) “Cybersecurity and Data Laws of the Commonwealth”, Springer.

Lima, C. V. G. (2021) “Crimes cibernéticos: o lado obscuro da rede”, PUC Goiás.

CERT.br. (2023) “Documentos e Whitepapers no cenário de ataques”. Disponível em: https://www.cert.br/docs/. Acesso em: 22 de dezembro de 2024.

Ramos, A. S. and Santos, J. O. (2022) “Cibercrime e sociedade: impactos e desafios”, Salvador: EDUFBA.

Cross, M. and Shinder, D. L. (2008) “Scene of the Cybercrime”, Syngress Pub.

Fórum Brasileiro de Segurança Pública. (2024) “18º Anuário Brasileiro de Segurança Pública”, São Paulo: Fórum Brasileiro de Segurança Pública. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/253. Acesso em: 22 de dezembro de 2024.

Lima, J. M. and Viana, J. R. (2024) “Crimes cibernéticos durante a pandemia: Impactos em crianças e adolescentes”. Disponível em: https://periodicorease.pro.br/rease/article/view/13976/6921. Acesso em: 21 de dezembro de 2024.

Jornal da USP. (2023) “Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano”. Disponível em: https://jornal.usp.br/radio-usp/brasil-sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/. Acesso em: 21 de dezembro de 2024.

Al-Khater, W. et al. (2020) “The Impact of Cybercrime on Small and Medium Enterprises (SMEs): A Review”, Journal of Information Security and Applications, v. 54, p. 102568.

Syafitri, et al. (2022) “Cybersecurity Awareness and Behavior: A Review of the Literature”, International Journal of Advanced Computer Science and Applications, v. 13, n. 2, p. 123-135.

Aslan, Ozkan-Okay, M., Yilmaz, A. A. and Akin, E. (2023) “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions”, Electronics, v. 12, p. 1333. Disponível em: https://doi.org/10.3390/electronics12061333. London: Springer.

Kaspersky. (2023) “Relatório de Ameaças à Segurança Cibernética”. Disponível em: https://www.kaspersky.com/resource-center/threats/security-threats-reports. Acesso em: 15 de dezembro de 2024.

Revista Forense Digital. (2023) “A evolução dos crimes cibernéticos e os desafios da legislação brasileira”. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 21 de dezembro de 2024.

Kumar, R., Sharma, S., Vachhani, C. and Yadav, N. (2022) “What changed in the cyber-security after COVID-19?”, Computers & Security, v. 120. Disponível em: https://doi.org/10.1016/j.cose.2022.102821. Acesso em: 10 de março de 2025.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021) “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic”, Computers & Security, v. 105. Disponível em: https://www.sciencedirect.com. Acesso em: 10 de março de 2025.