Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Departamento de Administração (ADM) Programa de Pós-Graduação em Administração (PPGA) MBA em Gestão e Governança em Segurança Pública

SARA – Inovação Tecnológica na Segurança Pública - Desenvolvimento e Implantação de um Sistema de Alerta Referencial Anonimizado para o Estado de Goiás

Orientandos: LÍVIA CRISTINA PONTES DE ARAÚJO,
RACKELL MARQUES DA S. OLIVEIRA,
YASSER MARTINS YASSINE

Prof. Orientador Dr. Thiago Gomes Nascimento

BRASILIA – DF
2025

Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Departamento de Administração (ADM) Programa de Pós-Graduação em Administração (PPGA) MBA em Gestão e Governança em Segurança Pública

SARA – Inovação Tecnológica na Segurança Pública - Desenvolvimento e Implantação de um Sistema de Alerta Referencial Anonimizado para o Estado de Goiás

Orientandos: LÍVIA CRISTINA PONTES DE ARAÚJO, RACKELL MARQUES DA S. OLIVEIRA, YASSER MARTINS YASSINE

Trabalho de Conclusão de Curso de Pós-Graduação/MBA em Gestão e Governança de Segurança Pública, da Universidade de Brasília, como requisito à obtenção do título de Especialista em Gestão e Governança de Segurança Pública.

BRASILIA – DF
2025

Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Departamento de Administração (ADM) Programa de Pós-Graduação em Administração (PPGA) MBA em Gestão e Governança em Segurança Pública

SARA – Inovação Tecnológica na Segurança Pública - Desenvolvimento e Implantação de um Sistema de Alerta Referencial Anonimizado para o Estado de Goiás

Trabalho de Conclusão de Curso defendido, em Sessão Pública, e aprovado pela Banca Examinadora, composta pelos seguintes membros avaliadores:

Prof. Dr. Thiago Gomes Nascimento – Orientador

Prof. Dr. Francisco Antônio Coelho Júnior – Membro Interno – UNB – MBA Gestão e Governança Pública.

Prof. Dr. Breno Giovanni Adaid Castro – Membro Externo – IDP.

BRASILIA – DF
2025

RESUMO

O presente trabalho acadêmico aborda o desenvolvimento e a implementação de uma plataforma/aplicativo denominado SARA, que significa Sistema de Alerta Referencial Anonimizado, o que indica uma inovação tecnológica voltada para a Segurança Pública do Estado de Goiás, podendo ser expandido nacionalmente. O SARA é concebido como uma ferramenta eficiente para o combate ao estelionato virtual e outras fraudes digitais, problemas crescentes que ameaçam a segurança e os direitos humanos de quinta geração, como a privacidade e a proteção de dados. A pesquisa contextualiza o cenário atual da segurança digital, evidenciando a necessidade de sistemas integrados e anônimos que permitam a rápida comunicação entre vítimas, órgãos de segurança pública e instituições financeiras, sem expor dados pessoais ou comprometer a investigação. A proposta do SARA integra tecnologias como sistema de busca e análise de dados, algoritmos preditivos e sistemas de alerta automatizado, permitindo maior eficiência no registro, análise e disseminação de informações sobre fraudes em tempo real. A implementação do sistema é discutida em etapas, desde o planejamento e desenvolvimento tecnológico até a fase de implantação e monitoramento pela Segurança Pública. Também são abordados os desafios enfrentados, como os custos para implementação, a capacitação dos agentes envolvidos e a compatibilidade com a legislação vigente, como a Lei Geral de Proteção de Dados (LGPD). O trabalho conclui que o SARA representa um avanço significativo para a gestão da segurança pública em Goiás, promovendo maior agilidade, precisão e cooperação no enfrentamento do crime digital, ao mesmo tempo em que reforça a confiança da sociedade nas instituições responsáveis pela garantia da segurança e dos direitos fundamentais. Após a implementação e análise dos indicadores de qualidade, o SARA pode ser expandido a nível nacional, integrando os diferentes Estados e possibilitando toda população brasileira a ser usuário da plataforma/aplicativo. O projeto contempla sua implementação primeiramente no Estado de Goiás em razão de dois dos autores deste trabalho serem integrantes da Polícia Civil desse Estado, contudo traz exemplos do Estado do Amapá, uma vez que a terceira integrante é ocupante de cargo de Delegada de Polícia naquele Estado.

Palavras-Chave: Segurança Pública, Fraudes Digitais, Inovação Tecnológica, Proteção de Dados, Cibercrime.

ABSTRACT

The present academic work discusses the development and implementation of a platform/application called SARA, which stands for Anonymized Referential Alert System. This initiative represents a technological innovation aimed at enhancing Public Security in the State of Goiás, with the potential for national expansion. SARA is designed as an efficient tool to combat virtual fraud and other digital scams, which are growing threats to security and fifth-generation human rights, such as privacy and data protection. The research contextualizes the current landscape of digital security, highlighting the need for integrated and anonymized systems that enable rapid communication between victims, public security agencies, and financial institutions without exposing personal data or compromising investigations. SARA's proposal incorporates technologies such as data search and analysis systems, predictive algorithms, and automated alert mechanisms, allowing for more efficient registration, analysis, and dissemination of information on fraud in real time. The system's implementation is discussed in stages, from planning and technological development to its deployment and monitoring by Public Security authorities. The study also addresses challenges such as implementation costs, training of involved personnel, and compliance with existing legislation, including the General Data Protection Law (LGPD). The research concludes that SARA represents a significant advancement in public security management in Goiás, promoting greater agility, accuracy, and collaboration in combating digital crime while reinforcing public trust in the institutions responsible for ensuring safety and fundamental rights. After implementation and quality indicator analysis, SARA has the potential to be expanded nationwide, integrating various states and enabling the entire Brazilian population to access and benefit from the platform/application. The project envisions its initial implementation in the State of Goiás, as two of the authors of this work are members of the Civil Police of that state. However, it also includes examples from the State of Amapá, given that the third author holds the position of Police Chief in that state.

Key-words: Public Security, Digital Fraud, Technological Innovation, Data Protetion, Cybercrime.

LISTA DE ABREVIATURAS

ANPP – Acordo de Não Persecução Penal

CEF – Caixa Econômica Federal

CNPJ – Cadastro Nacional de Pessoa Jurídica

CPF – Cadastro de Pessoa Física

DETRAN/AP – Departamento Estadual de Trânsito do Estado do Amapá

EUA – Estados Unidos da América

FBI - *Federal Bureau of Investigation*, cuja sigla traduzida para português significa Departamento Federal de Investigação

IA – Inteligência Artificial

IC3 – Internet Crime Complaint Center

IP – Endereço de Protocolo de Internet

LGPD – Lei de Garantia de Proteção de Dados – Lei Federal nº 13.709/2018

PIX – sistema de pagamentos instantâneos criado pelo Banco Central do Brasil (BCB)

PF – Policia Federal

RAI – Registro de Atendimento Integrado

SARA – Sistema de Alerta Referencial Anonimizado

SUMÁRIO

1. INTRODUÇÃO

A modernização dos sistemas de segurança pública é uma necessidade crescente para aprimorar o combate à criminalidade e oferecer uma resposta mais ágil à sociedade. Nesse contexto, o projeto de implementação da plataforma SARA (Sistema de Alerta Referencial Anonimizado) visa fornecer à população do Estado de Goiás um aplicativo para dispositivos móveis (Android e iOS) que permita o registro e o acesso a alertas de segurança.

A plataforma, a ser desenvolvida pela Secretaria de Segurança Pública do Estado de Goiás (SSP/GO) em primeiro momento, buscará estabelecer uma comunicação ágil e eficiente entre o cidadão e a polícia, promovendo maior transparência e controle sobre as informações de segurança.

É de conhecimento empírico que a COVID-19 trouxe grande aumento dos índices de criminalidade, especialmente fraudes e estelionatos eletrônicos, fato que continuou em ascensão também no período pós-pandemia até os dias atuais. Nesse sentido mostra pesquisa realizada pelo Anuário Brasileiro de Segurança Pública[1], afirmando que o número de estelionatos no Brasil mais que quadruplicou nos últimos cinco anos: em 2022, foram registrados 1.819.409 casos do crime, 326% a mais que em 2018, quando ocorreram 426.799 registros.

- Foram 151,6 mil casos por mês;
- Quase 5 mil casos por dia;
- 208 golpes por hora;
- E cerca de 3,5 registros de estelionato por minuto no ano passado de 2023;
- O aumento foi de 38,5% nos últimos dois anos, já que em 2021 foram 1.312.964 casos.

É entendimento do estudioso Chaves (apud SILVA, 2003, p.19), que Cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação". Desta forma, diante do conceito analítico de crime, conclui-se que "crimes cibernéticos" são todas as condutas "típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática" (SCHMIDT, 2014, [n.p.]).

Nesse sentido, é importante destacar o entendimento do CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2023)[2], conceituando o que é Fraude

---

[1] Os dados são do Anuário Brasileiro de Segurança Pública 2023, uma pesquisa feita pelo **Fórum Brasileiro de Segurança Pública** (FBSP). https://g1.globo.com/sp/sao-paulo/noticia/2023/07/20/estelionatos-no-brasil-mais-que-triplicam-em-cinco-anos-e-golpes-virtuais-disparam-apos-pandemia-revela-anuario.ghtml

[2] CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha.

Eletrônica. Segundo PAULO LIMA (2005) “A fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.”

Ainda conclui PAULO LIMA (2005) que fraudes virtuais sejam “a invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.”

No Brasil, os crimes cibernéticos tiveram sua ascensão com a Lei Federal n.º 12.737/2012 denominada Lei Carolina Dieckmann, muito antes do período pandêmico, no contexto de sequestro de dados através de invasão de dispositivo eletrônico por hackers. Somente no ano de 2021, no auge da Pandemia, é que o direito penal inovou com a publicação da Lei 14.155, de 27/05/2021, que alterou o Código Penal e acrescentou ao artigo 171 os parágrafos 2°-A e 2°-B relativos à fraude eletrônica, cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, ou por qualquer outro meio fraudulento análogo.

É de grande importância destacar, que no Estado de Goiás, a diminuição dos demais crimes patrimoniais, como roubo e furto de veículos, de cargas, em residências, roubo em estabelecimento bancários e comerciais, e até mesmo crimes de novo cangaço, diminuíram significativamente nos últimos anos. Segundo o Observatório de Segurança Pública do Estado de Goiás, entre janeiro e março de 2024 (comparação com o período de janeiro/março de 2023), os indicadores criminais desses crrimes diminuíram da seguinte forma:

- Roubo de Carga: -92%
- Furto a Transeunte: -34%
- Roubo em Comércio: -34%
- Roubo de Veículos: -34%
- Roubo a Transeunte: -33%
- Feminicídio: -31%

- Furto de Veículos: -27%
- Homicídio Doloso: -24%
- Furto em Residência: -20%
- Roubo em Propriedade Rural: -20%
- Furto em Comércio: -16%
- Roubo em Residência: -14%
- Tentativa de homicídio: -10%
- Estupro: -9%
- Furto em Propriedade Rural: -6%

A nível de Brasil, pode-se destacar o Anuário Brasileiro de Segurança Pública (2024, p. 15), que informa que "crimes de rua caem e estelionatos crescem", informando a cifra preocupante de 1 (um) golpe a cada 16 segundos.

Figura 1

Fluxograma estatístico do aumento de crimes de estelionato no Brasil e diminuição dos demais crimes patrimoniais.

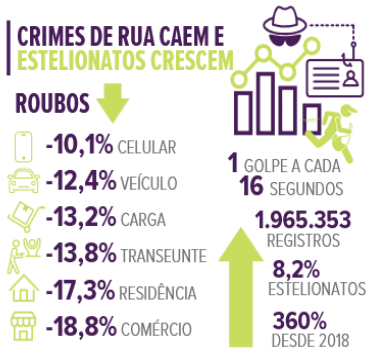


*Imagem extraída do Anuário Brasileiro de Segurança Pública (2024, p. 15) disponível em https://forumseguranca.org.br/wp-content/uploads/2024/07/anuario-2024.pdf acesso em 29/12/2024.

Isso não significa que a criminalidade tenha diminuído de modo geral, e que autores de crimes foram ressocializados. Pelo contrário, as estatísticas concluem que os criminosos migraram para uma nova forma de obter vantagem patrimonial ilícita, que é o estelionato, onde muitas vezes, ausente risco de morte concreto (confrontos policiais), utilizando smartphones na palma da mão, no conforto de suas residências; com gastos econômicos diminuídos em razão de logísticas e comparsas, podendo ser realizados até mesmo dentro de penitenciárias. Também verifica-se dos

trabalhos policiais realizados, que os crimes de estelionato estão financiando os crimes de tráfico de drogas.

Além do mais, o crime de estelionato é considerado de médio porte, não tem natureza de hediondo, podendo ser aplicado benefícios processuais como Acordos de Não Persecução Penal – ANPP e ainda, sem olvidar, que a natureza da ação é pública condicionada à representação. Desta forma, a punição estatal para os autores desse tipo de crime é bastante remota, sem esquecer das dificuldades para a investigação policial e as várias formas de burlar os sistemas. Todos esses fatores geram a convicção de que "o crime compensa".

Partindo da premissa, ao invés de melhorar os mecanismos de ação policial, que é matéria bastante estudada pelos estudiosos de segurança pública, o presente trabalho traz a importância da conscientização da população, na tentativa de prevenir a ocorrência de crimes dessa natureza, dificultando a ação dos criminosos, verificar o impacto social dos crimes, e garantindo melhores condições de vida e segurança, bem como aumentar a sensação de segurança no mundo digital.

Diante desse quadro torna-se fundamental o desenvolvimento de uma plataforma que permita uma interação segura e rápida entre a população e a polícia, visando uma estrutura preventiva. A implementação do SARA visa justamente preencher essa lacuna, oferecendo uma interface digital que promove o cadastramento seguro do indivíduo, proporcionando uma solução acessível, com foco na prevenção e no combate a atividades ilícitas.

Um exemplo a ser destacado são os milhares de golpes de estelionato envolvendo empresas falsas e compra e venda *online*, onde a vítima sofre prejuízo. O RAI n.º 39816486**,** de fato ocorrido no Estado de Goiás, narra caso específico datado de 10/01/2025, onde a vítima contratou empresa *online* para aquisição de uniformes, e somente constatou o crime quando da não emissão de nota fiscal. Em entrevista, foi perguntado à vítima deste caso, se o projeto SARA já existisse quando da ocorrência do crime, se teria confiança em utilizá-lo, tendo respondido afirmativamente, bem como demonstrando total confiança nos avisos a serem retornados.

De igual forma, no Estado do Amapá, foi registrado o BO n.º 00003286/2025, pela 5ª Delegacia de Polícia de Macapá/AP, referente ao fato ilícito ocorrido em 14/01/2025, por meio do qual a vítima narrou ter sido vítima de golpe, envolvendo ofertas de produtos no *marketplace* da rede social *Facebook*. No aludido caso, a ofendida acreditou estar comprando eletrodomésticos e até contratou uma transportadora para fazer o frete dos produtos pelos quais pagou, só tendo percebido que se tratava de um golpe quando percebeu que fora bloqueada no aplicativo de

mensageria Whatsapp pelos infratores. Em sua entrevista, lamentou ainda não poder ter acesso a uma plataforma como o SARA e afirmou que, se tivesse recebido os alertas do sistema proposto, teria desistido da compra, evitando o golpe.

O SARA tem como escopo principal inovar no mundo virtual e na Segurança Pública, buscando meios preventivos e de orientação à população, de modo geral, evitando que pessoas sejam vítimas fáceis de crimes de estelionato virtual. Assim sendo, além da diminuição das estatísticas criminais acerca desse crime, contribuir com o impacto social e a saúde pública também são objetivos do projeto.

É importante destacar que além do prejuízo econômico, a vítima do crime de estelionato virtual sofre um abalo emocional e psicológico muito grande, sendo que em algumas vezes apresenta quadros de distúrbio de ansiedade, depressão, e em casos mais extremos até o autoextermínio. Nesse sentido, destaca-se caso ocorrido na capital do Estado de Goiás, narrado através do RAI n.º 36159899, onde a vítima cometeu suicídio logo após ter sido vítima de um golpe, sofrendo um prejuízo de aproximadamente meio milhão de reais.

A ideia é que, evitando a ocorrência do crime, além de ferramenta de inovação tecnológica, o SARA alcançará também vários fatores sociais e de saúde pública, evitando atendimentos médicos e hospitalares, contribuindo também para o Sistema Único de Saúde – SUS.

Segundo uma pesquisa realizada pela empresa de segurança Fortinet (2023), o Brasil é o segundo país mais impactado por crimes cibernéticos na América Latina. Os dados dão ciência de que foram cerca de 103,1 bilhões de tentativas de ataques apenas em 2022.

> “Desde 2013 o Brasil tem figurado como principal alvo na América Latina e como um dos países mais visados pelos criminosos digitais em todo o mundo. Para elevar o nível de proteção é fundamental que as organizações e empresas adotem soluções de segurança em multicamadas, para ampliar a visibilidade e a detecção de comportamentos suspeitos, e para terem resposta rápida no caso de invasões.” César Cândido, diretor geral da Trend Micro Brasil [3]

[3] disponível em https://olhardigital.com.br/2023/09/25/seguranca/brasil-e-o-segundo-pais-mais-vulneravel-a-ataques-hackers-diz-relatorio/ acesso em 31/01/2025

1.1 – Ferramentas utilizadas em outros Países;

Verifica-se que nos Estados Unidos da América – EUA, o FBI – Federal Bureau of Investigation, cuja sigla traduzida para português significa **Departamento Federal de Investigação,** criou uma plataforma digital, denominada IC3 - **Internet Crime Complaint Center[4],** permitindo a qualquer usuário registrar reclamação que envolva crimes cibernéticos. Nela, o Governo Americano afirma que "precisa" da população para mapear e tentar diminuir os crimes de estelionato virtual.

Na plataforma é informado que as denúncias direcionadas, combinadas com outros dados, permite ao FBI investigar crimes relatados, rastrear tendências e ameaças e, em alguns casos, até congelar fundos roubados. Tão importante quanto isso, o IC3 compartilha relatos de crimes em toda a sua vasta rede de escritórios de campo do FBI e parceiros de aplicação da lei, fortalecendo a resposta coletiva da nação norte-americana, tanto local quanto nacionalmente.

Devido ao grande número de reclamações, o IC3 não pode responder diretamente a todas as submissões, mas afirma que leva a sério cada relatório. A plataforma não permite que os usuários façam pesquisas, evitando a ocorrência de novos crimes, contudo é uma ferramenta de investigação policial que promove interação entre a população e as forças de segurança pública norte-americanas.

Também foi identificado nos Estados Unidos da América, outra plataforma interativa entre Segurança Pública e população. Através do Lee County Sheriff's Office[5], localizada no Condado de Lee, é possível que cidadãos realizem pesquisa sobre a situação de um determinado preso. O Gabinete do Xerife do Condado de Lee é uma agência de aplicação da lei multifacetada, responsável principalmente pelos serviços de aplicação da lei no condado de Lee não incorporado, além da cidade de Bonita Springs, da vila de Estero e da cidade de Fort Myers Beach. Os deputados têm jurisdição em todo o condado e também fornecem serviços de aplicação da lei secundária dentro dos limites das cidades de Fort Myers, Cape Coral e Sanibel.

Essa plataforma tem como missão salvaguardar vidas e bens; aplicar respeitosamente as leis do país e trabalhar cooperativamente para diminuir o impacto do crime na vida dos residentes e visitantes do condado de Lee.

---

[4] Disponível em https://www.ic3.gov/ acesso em 31/01/2025
[5] Disponível em https://www.sheriffleefl.org/booking-search/ acesso em 31/01/2025

Muito embora com panoramas completamente diferentes, verifica-se que o Lee County Sheriff's Office guarda estreita consonância com o SARA, ou seja, ambos tem como objetivos salvaguardar vidas e bens; aplicar respeitosamente as leis do Brasil e trabalhar cooperativamente para diminuir o impacto do crime cibernético na vida da população de modo geral.

O uso de tecnologias no combate à criminalidade também tem avançado globalmente. Nos EUA, o uso de big data é destacado no estudo *"Leveraging Big Data Analytics to Combat Emerging Financial Fraud Schemes in the USA"*. A pesquisa demonstra como grandes volumes de dados estão sendo analisados para identificar padrões criminosos e realizar intervenções preventivas e estratégicas em fraudes financeiras (Smith & Johnson, 2023).

No Iraque, o artigo *"Crime Reporting and Police Controlling: Mobile and Web-Based Approach for Information-Sharing in Iraq"* aborda uma solução tecnológica que facilita a comunicação entre a população e as forças policiais por meio de uma plataforma móvel e web. A ferramenta promove denúncias anônimas e seguras, contribuindo para a reconstrução da confiança entre a sociedade e as forças de segurança em um contexto marcado por instabilidade política (Brown & Martinez, 2022).

Na Nigéria, o estudo *"Development of a Software System for Real-Time Management of Crime Reports in Southwestern Nigeria: The Administrative Approach"* descreve o desenvolvimento de um software que automatiza o registro de denúncias e permite o acompanhamento em tempo real das investigações. Essa solução foca na eficiência administrativa e na redução da burocracia, promovendo maior agilidade nas respostas policiais (Nguyen & Williams, 2022).

Nas Filipinas, destaca-se o aplicativo *Crimeline*, descrito no artigo *"Crimeline: Empowering Public Safety with GIS-Based Crime Incident Reporting"*. Desenvolvido pela Surigao Del Norte State University, o Crimeline utiliza tecnologia GIS (Sistema de Informação Geográfica) para permitir que cidadãos relatem crimes em tempo real, visualizem incidentes em mapas interativos e colaborem com as autoridades na análise de padrões criminais. Essa ferramenta promove maior engajamento comunitário e facilita a alocação eficiente de recursos pelas forças de segurança (Galila, 2023).

Essas iniciativas globais ilustram como a aplicação de tecnologias inovadoras pode aproximar as autoridades da população, otimizar recursos e fortalecer a prevenção ao crime.

Apesar de cada solução estar adaptada a contextos locais distintos, todas compartilham o mesmo objetivo: construir comunidades mais seguras e engajadas no combate à criminalidade.

2. FUNDAMENTAÇÃO TEÓRICA

A tecnologia tem desempenhado um papel transformador no enfrentamento da criminalidade, proporcionando ferramentas que aumentam a eficiência das forças de segurança, promovem a prevenção de crimes e melhoram a tomada de decisões estratégicas. Sua aplicação abrange diversas áreas, desde a análise de dados até a automação de processos, com impactos significativos em termos de vigilância, investigação e resposta rápida a incidentes.

De acordo com MIRANDA (2012) "Em 2003, a Secretaria Nacional de Segurança Pública (Senasp) do Ministério da Justiça explicitou o diagnóstico de que a carência de informações qualitativas e de análises consistentes sobre o cenário da segurança no país gerava um entrave à promoção da reestruturação institucional, à elaboração e à execução de políticas de combate à violência e à criminalidade. Para enfrentar a questão, a Senasp publicou um edital com as áreas prioritárias para investimentos em pesquisa em segurança e justiça criminal e promoveu investimentos na reestruturação do ambiente tecnológico, "particularmente no Sistema Integração Nacional de Informações sobre Justiça e Segurança (Infoseg), de modo a viabilizar a consolidação do Sistema Único de Segurança Pública (Susp)" (MIRANDA, 2012, p. 446)

A sociedade atual é uma sociedade de informação, onde todos os órgãos estão em constante evolução tecnológica. Trazendo para o contexto do tema, pode-se citar alguns principais impactos da tecnologia no combate à criminalidade:

a) Inteligência Artificial (IA) e Big Data:

A Inteligência Artificial (IA) e o Big Data permitem analisar grandes volumes de dados de forma rápida e precisa, identificando padrões e tendências criminais, facilitando fatores como a previsão de crimes e identificação de suspeitos, como ferramentas de reconhecimento facial e biometria que auxiliam na identificação de indivíduos em tempo real.

b) Comunicação e Compartilhamento de Informações:

Aplicativos e plataformas digitais facilitam a comunicação entre os cidadãos e as forças de segurança, como o SARA que visa promover o anonimato e a agilidade no recebimento de informações.

Integração de bases de dados através de sistemas interconectados entre diferentes órgãos permitindo acesso rápido a informações relevantes, como antecedentes criminais e dados de veículos.

c) Investigação e Análise Digital

Ciberinvestigações são ferramentas especializadas que rastreiam atividades ilícitas na internet, incluindo redes sociais e *dark web*.

Análise forense digital: Identifica evidências eletrônicas em dispositivos e redes, essenciais para casos de crimes virtuais.

O impacto da tecnologia no enfrentamento da criminalidade é profundo, modificando tanto a maneira como os crimes são cometidos, quanto às estratégias utilizadas para preveni-los e combatê-los. Em um mundo cada vez mais digital, a integração de ferramentas tecnológicas tem transformado a segurança pública, oferecendo soluções inovadoras para problemas antigos e novos desafios.

2.1 – A Privacidade e o anonimato como garantia de proteção de dados.

O sistema SARA tem como objetivo implementar técnicas avançadas de anonimização, que tornam os dados impossíveis de serem associados diretamente a indivíduos. Isso atende ao Art. 12 da Lei Federal n° 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), cuja qual determina que dados anonimizados não são considerados dados pessoais desde que o processo de anonimização não seja reversível.

Ainda poderá transformar dados identificáveis (nome, CPF, endereço) em identificadores irreversíveis (*hashes, tokens* ou pseudônimos) antes de serem processados, garantindo que informações sensíveis sejam protegidas.

Ademais, o próprio art. 4º, LGPD, em todas as alíneas do inciso III, prevê finalidade para ações de segurança pública e investigação e repressão de infrações penais.

O SARA deve adotar políticas de governança claras, com mecanismos a observar o *accountability*, como registro de logs (manter registros de quem acessa ou utiliza os dados do sistema, garantindo rastreabilidade e conformidade) e relatórios de Impacto (documenta e avalia os riscos de privacidade relacionados ao uso do sistema).

Também deve implementar políticas de retenção de dados, armazenando informações somente pelo tempo necessário para cumprir sua finalidade, conforme previsto na LGPD, de forma que poderá trabalhar com emissão de alertas, ou seja, após a emissão de alertas, os dados processados podem ser descartados, retendo apenas informações agregadas para análise estatística.

Contudo, em resumo, serão garantias de proteção de dados no SARA:

1. Proteção total do anonimato como prioridade (para os alertas).
2. Minimização e a propósito para dados coletados.
3. Criptografia e segurança nos processos.
4. Auditorias regulares e governança eficaz.
5. Base legal robusta para tratamento de dados.

Primeiramente convém destacar, que o Direito à Proteção de Dados foi recentemente incluído como direito fundamental da pessoa humana, nos termos da Emenda Constitucional n.º 115/2022, permitindo maior segurança jurídica no país aos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD). Conforme disposto no artigo 1º da LGPD, a lei visa proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural.

O respeito à LGPD é essencial para o funcionamento do SARA, garantindo a conformidade legal e a proteção de direitos fundamentais. O SARA assegura que nenhum dado protegido será divulgado, limitando-se ao uso de dados quantificados, tratados de forma anonimizada e em consonância com o artigo 12 da LGPD, que exclui dados anonimizados da aplicação da referida lei, desde que não possam ser revertidos para identificar o titular.

Lei 13.709/2008.

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

O SARA alinha-se aos princípios fundamentais previstos no artigo 2º da LGPD, especialmente os princípios da finalidade, necessidade e segurança, ao tratar apenas os dados estritamente necessários para garantir direitos fundamentais como a vida, saúde, segurança patrimonial e a proteção de um ambiente virtual seguro, enquadrando-se na hipótese de tratamento de dados para proteção da vida ou da incolumidade física de terceiros, conforme previsto no artigo 7º, inciso VII, e §3º da LGPD. A seguir texto legal:

Lei 13.709/2008.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

(...)

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

O objetivo primordial do SARA transcende a simples garantia de acesso à informação, voltando-se à salvaguarda de valores essenciais da pessoa humana, consagrados no artigo 1º, inciso III, da Constituição Federal de 1988, que estabelece a dignidade da pessoa humana como um dos fundamentos da República Federativa do Brasil. Além disso, está em harmonia com os compromissos internacionais assumidos pelo Brasil, como a Declaração Universal dos Direitos Humanos (Resolução 217 A III – em 10 de dezembro 1948), que protege a dignidade, liberdade e segurança das pessoas.

O artigo terceiro da Declaração Universal dos Direitos Humanos (1948) determina que "todo ser humano tem direito à vida, à liberdade e à segurança pessoal".

Em situações de eventual conflito entre os direitos fundamentais, a proteção de dados e outros direitos, deve-se observar o princípio da proporcionalidade, amplamente reconhecido no ordenamento jurídico brasileiro e implícito no artigo 5º, §2º, da Constituição Federal, sendo uma decorrência do Estado de Direito e, portanto, o limite da atuação estatal no que tange ao exercício do poder de restringir direitos, principalmente, direitos e garantias fundamentais.

Tal princípio atua como complemento do princípio da razoabilidade, tendo como alvo a conquista do equilíbrio necessário à concretização da justiça efetiva, guardando observância aos direitos garantidos constitucionalmente. A proporcionalidade tem efeito regulador na aplicação dos demais princípios constitucionais, no intuito de evitar que se dê muita importância a um ou outro princípio, em detrimento de outro igualmente importante.

Como acertadamente afirma Paulo Vaz (2002), "Diante da colisão de princípios, é preciso verificar qual dos princípios possui maior peso diante das circunstâncias concretas." E, segundo o mesmo autor, a proporcionalidade "[...] irá definir os critérios de delimitação da relação meio-fim, assegurando a restrição na exata medida do necessário e evitando excessos. Vai salvar o núcleo essencial do direito tutelado pelo princípio relativizado".

Finaliza Paulo Vaz (2002), que, proporcionalidade e razoabilidade constituem vertentes ou dimensões do princípio do devido processo legal e, voltadas, para o direito material e vocacionadas ao aperfeiçoamento dos ideais de justiça que norteiam os julgamentos do Poder Judiciário.

Assim, quando colocados em contraposição, direitos fundamentais como a vida, saúde, segurança e dignidade humana devem possui maior peso em detrimento do direito a proteção de dados, em razão da proeminência dos primeiros em desfavor do segundo. Portanto, a operacionalização do SARA visa uma forma ética, legal e orientada à proteção dos direitos fundamentais, assegurando que sua aplicação esteja sempre em consonância com a Constituição Federal de 1988, a LGPD e os tratados internacionais que promovem e protegem os direitos humanos.

Além do mais, o estelionato digital, como manifestação do medo do crime no ambiente virtual, conecta-se diretamente com os direitos humanos de 5ª geração ao destacar a importância da segurança digital, do acesso igualitário à tecnologia e da cooperação internacional para a proteção dos usuários. Enfrentar esses desafios é fundamental para garantir um ambiente digital seguro e equilibrado, onde os direitos de privacidade e segurança sejam plenamente respeitados.

2.2 – Impacto Social dos Crimes de Estelionato Virtual;

O presente trabalho inspirou a realização de uma pesquisa entre pessoas nos Estados de Goiás e Amapá, tendo revelado que 92,8% (noventa e dois virgula oito porcento) dos entrevistados informaram ter conhecimento sobre fraudes eletrônicas, o que demonstra que o crime virtual é um problema amplamente reconhecido, afetando grande parte da população.

Além disso, um número significativo de pessoas já foram vítimas de crimes de estelionato, alguns mais de uma vez inclusive, o que indica claramente que não é apenas uma ameaça teórica, mas uma realidade concreta, cuja qual causa impactos financeiros e emocionais, atingindo as mais variadas áreas da vida. Quando perguntados sobre os impactos do estelionato, os participantes mencionaram prejuízos financeiros, emocionais e sociais, destacando-se as seguintes queixas: vergonha de relatar o golpe; medo e insegurança para realizar novas transações financeiras; abalos emocionais significativos – incluindo ansiedade e depressão; perdas financeiras consideráveis, afetando a estabilidade das vítimas.

O SARA vem para modificar o cenário da segurança pública no Estado de Goiás, e posteriormente, em todo o Brasil, haja vista que não apenas previne fraudes, mas também busca um impacto social positivo, com a redução de danos emocionais e financeiros às vítimas, contribuindo para a saúde pública e minimizando o estresse psicológico causado pelos golpes.

Desta forma, está clarividente a urgência de um sistema de prevenção e alerta, que possa informar aos cidadãos, em tempo real, sobre possíveis fraudes, tentando reduzir a ocorrência desses crimes e gerar maior confiabilidade no sistema de segurança pública.

3. OBJETIVOS

A presente pesquisa tem como objetivo principal a entrega de um aplicativo/plataforma, denominado SARA – Sistema de Alertas Referencial Anonimizado, capaz de garantir aos usuários os seguintes benefícios:

3.1 Aplicativo gerenciável, através de utilização por *login* e senha, onde o usuário poderá ter acesso quantitativo às ocorrências policiais instauradas a partir de um dado trazido por si próprio;

3.2 Pesquisas quantitativas, que retornam alertas anonimizados, de possíveis situações policiais envolvendo o dado pesquisado. Os Alertas serão em cores – verde para pouca possibilidade de golpe; amarelo para possível situação de golpe; vermelho para efetiva situação de golpe; e vermelho com sinal sonoro, alertando o usuário a procurar maiores informações fidedignas sobre o dado pesquisado.

3.3 Orientações em tempo real, diretas, simples e claras, conduzindo o usuário a um atendimento pessoal e personalizado, indicando o endereço da Delegacia de Polícia mais próxima, e/ou conduzindo-o para registro de ocorrência policial *online*, em casos em que o usuário tenha sido vítima de crimes de estelionato digital e/ou outras fraudes;

3.4 Vídeos explicativos, dinâmicos, sobre a engenharia utilizada pelos golpistas, indicando possíveis fatos que podem configurar crimes, e orientando os usuários para que não sejam vítimas fáceis de tais golpes, possibilitando também contato em tempo real através de chat.

3.5 Campanhas educacionais;

É de bom alvitre destacar que um dos objetivos essenciais do SARA é promover a educação e conscientização da população sobre o correto uso e manuseio da plataforma. O sucesso de um sistema digital não depende apenas de sua eficácia técnica, mas também da adesão e compreensão dos usuários em relação às suas funcionalidades, segurança e benefícios. Nesse contexto, a realização de campanhas educativas torna-se uma estratégia fundamental para sensibilizar e orientar os usuários sobre como tirar proveito da ferramenta de maneira segura e eficiente.

Verifica-se que, muitas vezes, a falta de interesse da população em se informar sobre o tema está diretamente relacionada à baixa percepção da relevância do assunto ou até mesmo à falta de compreensão sobre os riscos envolvidos. A natural resistência ao aprendizado sobre novas tecnologias é um fenômeno comum, especialmente quando se trata de sistemas complexos ou quando não se percebe de imediato a necessidade de adquirir tais conhecimentos. Nesse cenário, o uso de táticas de *marketing* eficazes é uma abordagem necessária para atrair a atenção do público-alvo e despertar o interesse sobre o assunto.

As campanhas educativas, quando bem planejadas, podem criar uma conexão com os usuários, oferecendo conteúdos relevantes e acessíveis, que abordem de forma simples e clara os aspectos mais importantes sobre o uso do aplicativo. É importante que essas campanhas não apenas informem sobre as funcionalidades do sistema, mas também ressaltem a importância da segurança digital, destacando os riscos de golpes e fraudes no ambiente *online*. Ao educar a população sobre os tipos de golpes mais comuns, o projeto não só instrui o usuário, mas também o capacita a reconhecer sinais de fraude e adotar comportamentos preventivos.

Além disso, as campanhas devem ser realizadas de forma a alcançar diferentes segmentos da população, utilizando canais de comunicação variados, como redes sociais, sites especializados, vídeos explicativos e até mesmo eventos presenciais, caso possível. A linguagem utilizada deve ser simples, clara, objetiva e inclusiva, de modo que todos, independentemente do seu nível de conhecimento em tecnologia, possam compreender a mensagem.

Governos de países como Estados Unidos, Canadá e Austrália têm promovido campanhas de conscientização pública para alertar cidadãos sobre golpes comuns, como: Golpe do falso sequestro: quando criminosos ligam para familiares exigindo resgates. Golpe do falso boleto: fraude em que golpistas se passam por bancos ou empresas de cobrança. Os três países investem fortemente em educação digital, alertas de fraudes e tecnologias para mitigar golpes virtuais. Enquanto os EUA focam em divulgação massiva de alertas e políticas de segurança digital, o Canadá aposta em prevenção contínua e centralização de denúncias. Já a Austrália se destaca por um monitoramento ativo de golpes e pela parceria com entidades internacionais para combater crimes digitais.

Tabela 1. Campanhas educativas para prevenção de crimes de estelionato digital e outros, nos países Estados Unidos da América, Canadá e Austrália:

Estados Unidos da América – EUA	Canadá	Austrália
Campanha "Stop. Think. Connect." Criada pelo Departamento de Segurança Interna dos EUA (DHS) em parceria com empresas e ONGs, essa campanha tem o objetivo de educar os cidadãos sobre segurança online e golpes digitais. Foca em alertar sobre fraudes bancárias, phishing e engenharia social, incentivando as pessoas a verificar e confirmar antes de clicar ou fornecer dados pessoais. É amplamente divulgada em redes sociais, escolas e locais públicos. Site oficial: Stop. Think. Connect.[6]	**"Fraud Prevention Month" – Mês de Prevenção a Fraudes** O governo canadense, por meio do Competition Bureau, realiza todos os anos uma campanha nacional de prevenção contra fraudes digitais. Em parceria com bancos e empresas de tecnologia, divulga informações sobre os principais golpes e ensina os cidadãos a reconhecer sinais de fraude. Site oficial: Fraud Prevention Month[7]	**"Scamwatch" – Comissão Australiana de Concorrência e Consumidor (ACCC)** Plataforma do governo australiano para monitoramento e alerta sobre fraudes digitais. Acompanha os principais golpes ocorrendo no país e fornece dados estatísticos sobre o impacto dos golpes financeiros. Publica guias sobre como evitar fraudes bancárias, phishing e golpes de chamadas falsas. Site oficial: Scamwatch[8]
"FTC Consumer Alerts" – Comissão Federal de Comércio (FTC)	**"Get Cyber Safe" – Governo do Canadá**	**"Stay Smart Online" – Governo da Austrália**

[6] Stop. Think. Connect. https://www.stopthinkconnect.org/
[7] *Site oficial:* [Fraud Prevention Month](https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04385.html)
[8] Scamwatch – Australian Competition and Consumer Commission (ACCC) https://www.scamwatch.gov.au/

A Federal Trade Commission (FTC) mantém uma seção de alertas de fraudes onde publica avisos regulares sobre novos golpes virtuais. Destaca fraudes como o golpe do falso sequestro e golpes bancários, fornecendo orientações sobre como agir caso alguém seja alvo. Os cidadãos podem reportar golpes e receber alertas sobre fraudes em tempo real. Site oficial: FTC Consumer Alerts[9]	Uma iniciativa do governo canadense para educar cidadãos e empresas sobre golpes virtuais e segurança digital. Fornece materiais educativos sobre fraudes bancárias e phishing, além de ensinar como criar senhas seguras e evitar ataques de engenharia social. Site oficial: Get Cyber Safe[10]	Campanha educacional sobre segurança digital e prevenção de golpes. Ensina como proteger informações bancárias e identificar tentativas de fraudes via telefone e e-mail. Promove alertas regulares sobre golpes emergentes. Site oficial: Stay Smart Online[11]
Campanha "Be Cyber Smart" Realizada durante o Mês Nacional da Cibersegurança, promovida pelo CISA (Cybersecurity and Infrastructure Security Agency) e a National Cyber Security Alliance. Encoraja práticas seguras online, como o uso de autenticação de dois fatores	**"Canadian Anti-Fraud Centre (CAFC)" – Centro Canadense Antifraude** Plataforma onde cidadãos podem relatar golpes como o do falso boleto e sequestro virtual. Atua em parceria com a Real Polícia Montada do Canadá (RCMP) e o Competition Bureau. Site oficial: Canadian Anti-Fraud Centre[13]	**"No More Ransom" – Polícia Federal Australiana (AFP)** Programa global de combate a ransomwares e outros tipos de golpes digitais. Criado em parceria com a Europol e diversas empresas de cibersegurança para fornecer ferramentas gratuitas de descriptografia para vítimas de ataques digitais.

[9] FTC Consumer Alerts – Comissão Federal de Comércio (FTC) https://www.consumer.ftc.gov/scams
[10] Get Cyber Safe – Governo do Canadá https://www.getcybersafe.gc.ca/en
[11] Stay Smart Online – Governo da Austrália https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online
[13] Canadian Anti-Fraud Centre (CAFC) https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

(2FA) e a evitação de chamadas suspeitas. Site oficial: Be Cyber Smart[12]		Site oficial: No More Ransom[14]

Essas iniciativas desempenham um papel fundamental na redução das vítimas de fraudes, promovendo o conhecimento e a prevenção contra crimes que afetam milhares de pessoas diariamente.

No Brasil, onde os golpes digitais e presenciais têm se tornado cada vez mais sofisticados, é essencial que o governo também invista em campanhas educativas voltadas para a população. Golpes como o falso sequestro, no qual criminosos ligam para familiares exigindo resgates, e o falso boleto, em que fraudadores se passam por instituições bancárias ou empresas de cobrança, são apenas alguns exemplos de práticas que causam prejuízos financeiros e emocionais para as vítimas.

A ausência de uma conscientização nacional estruturada permite que essas fraudes continuem a fazer vítimas, especialmente entre os mais vulneráveis, como idosos e pessoas com menos acesso à informação. O SARA é um projeto que viabiliza o país a investir em meios para educação digital e financeira, incluindo vídeos instrutivos, campanhas, cartilhas, anúncios e parcerias com instituições bancárias e de segurança pública para instruir os cidadãos sobre como identificar e evitar golpes.

Além disso, traz a implementação de um sistema eficiente de denúncia e suporte às vítimas, sendo um meio crucial para combater essas práticas criminosas. A tecnologia deve ser uma aliada nesse processo, permitindo alertas rápidos e eficazes sobre novas modalidades de golpes em circulação.

Com um esforço conjunto entre governo, empresas e sociedade civil, é possível criar uma cultura de prevenção e segurança, reduzindo significativamente o impacto dos golpes e aumentando a proteção dos cidadãos brasileiros contra fraudes. A informação é a melhor arma contra os criminosos, e a Segurança Pública investir em sua disseminação para garantir um país mais seguro para todos.

[12] Be Cyber Smart – Cybersecurity & Infrastructure Security Agency (CISA) https://www.cisa.gov/be-cyber-smart
[14] No More Ransom – Polícia Federal Australiana (AFP) https://www.nomoreransom.org/en/index.html

Portanto, o sucesso de um projeto que visa a utilização de um aplicativo depende não apenas da sua funcionalidade, mas também da capacidade de envolver a população e de educá-la sobre a importância da plataforma. A combinação de ações educativas, com o uso de estratégias de *marketing* para atrair a atenção dos interessados, é fundamental para promover a conscientização, prevenir golpes e garantir que o público faça uso do sistema de maneira segura e responsável.

Em relação aos indicadores de sucesso, verifica-se que são essenciais para avaliar o impacto e a eficácia do projeto ao longo do tempo. Eles permitem medir a adesão dos usuários, a efetividade das campanhas educativas e a capacidade da plataforma de alcançar seus objetivos principais. A escolha dos indicadores corretos depende dos objetivos específicos do aplicativo, mas de maneira geral, podem ser divididos em categorias como engajamento, usabilidade, segurança e impacto social.

4. DESENVOLVIMENTO DO SARA

A criação e desenvolvimento do SARA por meio de aplicativo Android ou IOS possibilitará aos usuários cadastramento via *login* e senha, com especificação de dados pessoais como nome, documentos pessoais, endereço, telefone, com a finalidade de auditar a utilização da plataforma, permitindo o acesso somente para maiores de idade.

A plataforma/aplicativo deverá estar vinculada diretamente aos Registros de Atendimento Integrado – RAIs[15] elaborados para os crimes de estelionato, previstos em todas as modalidades do artigo 171 do Código Penal, e ainda, furto mediante fraude, tipo do artigo 155, § 4º, II do Código Penal e invasão de dispositivo – artigo 154-A, do Código Penal. Assim, quando for registrada uma ocorrência policial com essas tipificações, deverá ser vinculado automaticamente com a plataforma SARA.

Na ocorrência policial será importante que o registrador identifique corretamente o suposto autor do crime – com número de CPF ou CNPJ, bem como a pessoa que recebeu o valor indevido e as circunstâncias em que o crime ocorreu, em especial todas as informações materiais sobre o crime.

[15] RAI – Registro de Atendimento Integrado – é um documento utilizado por todos os órgãos da Segurança Pública do Estado de Goiás, para registro integrado entre as forças policiais de ocorrências policiais, evitando duplicidade e erros estatísticos. O RAI é um sistema integrado com a SENASP e a fonte primária de coleta de dados, análise criminal e informações estatísticas por parte da SSP-GO ainda em conformidade com a Portaria 229/2018 do MJ.

Recentemente, por trabalho desenvolvido pelo Titular do Laboratório de Análises Bancárias da Gerência de Operações de Inteligência da Polícia Civil do Estado de Goiás, está sendo introduzido pelo Observatório de Segurança Pública do Estado de Goiás, no campo específico "transações bancárias" dentro do RAI, a possibilidade de cadastrar chaves PIX, contas e agências bancárias, bem como informações que identifiquem as transações bancárias realizadas fraudulentamente e objeto de ocorrência policial. Essas informações irão viabilizar que a pesquisa seja fidedigna, e a busca de dados será conduzida pelas informações cadastradas no momento do registro do RAI.

Ainda constará na plataforma/aplicativo aba exclusiva disponibilizando vídeos institucionais curtos, confeccionados para orientar a população sobre os golpes de estelionato mais aplicados, bem como vídeos explicativos de campanhas orientativas, demonstrando através de vídeos animados os principais golpes que estiverem "na moda". Além do mais, constará vídeos explicativos de como proceder no caso da consumação do crime para relativização dos danos. A explanação por vídeos chama mais a atenção do público-alvo e leva a informação mais clara e precisa, facilitando, contudo, a comunicação com o usuário.

O usuário, devidamente cadastrado, informará o motivo da pesquisa e mediante a utilização de termos específicos, tais como: nome, CPF, CNPJ, chave PIX, número de telefone, poderá acessar resultados quantitativos, anonimizados, informando apenas a quantidade de ocorrências policiais registradas via RAI no Estado de Goiás, que tem como envolvido aquele termo utilizado. Não obstante, serão observados os ditames da Lei n.º 13.709/2018 – LGDP, que regulamenta a proteção de dados pessoais conforme já referido no item 1. Não será gerado relatório ou documento de pesquisa e as informações obtidas por esse meio não poderão ser elemento probatório em nenhum processo, seja cível, administrativo ou criminal.

Destaca-se que o cadastro e acesso ao sistema SARA não é anonimizado, devendo o usuário informar todos os seus dados, e inclusive indicar qual o motivo da pesquisa em campo próprio, facilitando que o sistema seja auditável pelos órgãos de Segurança Pública. É importante ficar claro que o SARA anonimiza os alertas emitidos diante de uma pesquisa, buscando, contudo proteger os dados dos envolvidos, tanto vítima quanto investigado, de forma que não será apresentada nenhuma informação vinculada à qualificação dos envolvidos, ou até mesmo acerca dos fatos que envolvam o crime em específico.

Convém ressaltar que o objetivo é exclusivamente preventivo e orientativo, visando orientar a população sobre os diversos tipos de golpes de estelionato que estão sendo aplicados nos dias atuais e prevenir para evitar o alastramento dos casos, permitindo que os usuários busquem informações em base de dados oficial, para que não sejam vítimas fáceis desses crimes.

5. METODOLOGIA

A metodologia para o desenvolvimento da plataforma SARA (Sistema de Alerta Referencial Anonimizado) foi planejada para garantir uma abordagem estruturada e eficiente, com etapas claras desde a análise inicial até as futuras fases de testes e implementação. O processo adota os princípios das metodologias ágeis, como o Scrum, para assegurar flexibilidade no desenvolvimento e alinhamento constante com os objetivos do projeto.

A primeira etapa foi a análise de requisitos, que consistiu na identificação das funcionalidades essenciais da plataforma em conjunto com a Secretaria de Segurança Pública do Estado de Goiás (SSP/GO), especialistas em tecnologia e segurança pública, e representantes da população-alvo. Essa etapa deve priorizar o levantamento de necessidades relacionadas à prevenção de cibercrimes, como o registro de ocorrências anônimas, o envio de alertas de segurança em tempo real e a proteção dos dados dos usuários, garantindo conformidade com a Lei Geral de Proteção de Dados (LGPD). Além disso, estudos de soluções internacionais, como, por exemplo, o IC3 nos EUA e o *Crimeline* nas Filipinas, cujos modelos forneceram insights valiosos para o escopo do projeto.

O desenvolvimento de um aplicativo envolve várias etapas, desde a concepção até a implementação e monitoramento contínuo. Abaixo estão os métodos e etapas comumente utilizados, com destaque para metodologias ágeis como o Scrum:

Tabela 2 – Análise de requisitos para implementação do SARA:

Análise de requisitos	
Objetivo	Compreender as necessidades do cliente e definir os requisitos do aplicativo.
Atividades	Reuniões com stakeholders para coletar informações.
	Definição de funcionalidades e restrições.

	Documentação dos requisitos funcionais e não funcionais.
Ferramentas	Entrevistas, questionários, brainstorming, diagramas de caso de uso.

Tabela 3 – Planejamento próprio para implementação do SARA:

Planejamento	
Objetivo	Estabelecer um plano de ação para o desenvolvimento do aplicativo.
Atividades	Definição do escopo do projeto
	Estimativa de tempo e custos.
	Seleção de metodologias de desenvolvimento (ex.: Scrum, Kanban)
	Definição de equipes e papéis.
Objetivo	Gráficos de Gantt, roadmap, matriz RACI.

Tabela 4 – Desenvolvimento do protótipo SARA – criação e desenvolvimento, implementação e testes:

Desenvolvimento do protótipo	
Objetivo	Criar uma versão inicial do aplicativo para validação de conceitos e funcionalidades.
Atividades	Desenvolvimento de wireframes e mockups.
	Implementação de funcionalidades básicas.
	Testes iniciais para validação de usabilidade.
Ferramentas	Ferramentas de design (ex.: Figma, Adobe XD), ambientes de desenvolvimento integrado (IDEs).

Tabela 5 – Desenvolvimento interativo e incremental para implementação do SARA:

Desenvolvimento interativo e incremental	
Objetivo	Desenvolver o aplicativo em ciclos curtos e iterativos, com entregas frequentes.
Atividades	Divisão do projeto em sprints (no caso do Scrum).
	Desenvolvimento de funcionalidades prioritárias.
	Revisões e ajustes contínuos com base no feedback.
Ferramentas	Scrum, Kanban, ferramentas de versionamento (ex.: Git), IDEs.

Tabela 6 – Fase de testes:

Testes	
Objetivo	Garantir a qualidade do aplicativo através de testes rigorosos.
Atividades	Testes unitários, de integração, de sistema e de aceitação.
	Identificação e correção de bugs.
	Validação de desempenho e segurança.
Ferramentas	Frameworks de teste (ex.: JUnit, Selenium), ferramentas de automação de testes.

Tabela 7 – Implementação Efetiva do SARA:

Implementação	
Objetivo	Disponibilizar o aplicativo para os usuários finais.
Atividades	Configuração do ambiente de produção.
	Implantação do aplicativo em lojas de aplicativos (ex.: Google Play, App Store) ou servidores.
	Migração de dados, se necessário.
Ferramentas	Ferramentas de CI/CD (Integração Contínua/Entrega Contínua), Docker, Kubernetes.

Tabela 8 – Monitoramento e manutenção do aplicativo já implementado:

Monitoramento e manutenção contínuos	
Objetivo	Garantir que o aplicativo continue funcionando corretamente e atenda às necessidades dos usuários.
Atividades	Monitoramento de desempenho e uso.
	Coleta e análise de feedback dos usuários.
	Implementação de atualizações e correções.
Ferramentas	Ferramentas de monitoramento (ex.: New Relic, Google Analytics), sistemas de suporte ao cliente.

Tabela 9 – Metodologias ágeis:

Metodologias ágeis	
Scrum	Papéis: Product Owner, Scrum Master, Equipe de Desenvolvimento.
	Artefatos: Product Backlog, Sprint Backlog, Incremento.
	Eventos: Sprint Planning, Daily Scrum, Sprint Review, Sprint Retrospective.
Kanban	Foco na visualização do fluxo de trabalho.
	Limitação do trabalho em progresso (WIP).
	Melhoria contínua do processo.

Verifica-se que as etapas incluirão testes e validação, programados para ocorrer após o término do desenvolvimento. Esses testes abrangerão a funcionalidade do sistema, sua usabilidade e a robustez das medidas de segurança. Grupos-piloto compostos por agentes de segurança pública e cidadãos serão envolvidos para fornecer feedback e identificar possíveis ajustes necessários. Após a validação, será iniciada a fase de implementação, que incluirá o lançamento gradual da plataforma e a realização de campanhas educativas para incentivar sua adesão pela população.

Por fim, a metodologia prevê um processo contínuo de monitoramento e atualização da plataforma após sua implementação. Serão coletadas métricas de desempenho, como a taxa de adesão e a incidência de cibercrimes, além de avaliações regulares da experiência dos usuários. A

conformidade com a LGPD continuará sendo uma prioridade, com políticas de anonimização de dados e auditorias periódicas para garantir a proteção e privacidade das informações coletadas.

A abordagem metodológica apresentada visa buscar, não apenas garantir a eficiência técnica do SARA, mas também sua relevância social, promovendo uma solução inovadora para o combate ao crescente número de cibercrimes no Estado de Goiás, e posteriormente em todo o país.

6. RESULTADOS ESPERADOS

O SARA tem como principal escopo buscar e alcançar resultados concretos e mensuráveis, alinhados aos objetivos de inovação tecnológica na segurança pública e sociais, visando à diminuição estatística de ocorrências policiais envolvendo crimes cibernéticos, de estelionato e outras fraudes, bem como atuar em parceria com as áreas de saúde pública e social, diminuindo índices de doenças psicológicas desencadeadas pela vitimização do cidadão.

Nesse diapasão, pode-se destacar, objetivamente, os resultados a seguir elencados:

6.1 – Redução dos Crimes de Estelionato

A implantação do SARA visa reduzir significativamente o índice de crimes de estelionato no Estado de Goiás. A natureza orientativa da plataforma visa informar aos cidadãos sobre a existência dos diversos golpes e a engenharia utilizada pelos golpistas, evitando que as vítimas sejam presas fáceis e obstando a consumação do crime.

O Estado utilizará das informações que possui, ou seja, das diversas ocorrências policiais que existem em seu banco de dados, para orientar as pessoas acerca dos riscos aos quais estão sujeitos, dando à população uma fonte confiável de consultas a registros de fraudes virtuais.

Ademais, espera-se que a interconexão do SARA com os Registros de Atendimento Integrado (RAIs) permita a utilização de dados históricos e projeções estatísticas por parte dos órgãos de segurança pública, de forma que possam identificar e mitigar práticas fraudulentas com maior rapidez e eficiência, uma vez que terão acesso a dados estatísticos e padrões criminais, possibilitando o melhor direcionamento das investigações.

Saliente-se, ainda, a diminuição da reincidência de golpes, uma vez que infratores que costumam utilizar os mesmos métodos (*modus operandi*) repetidamente terão dificuldade de ludibriar novas vítimas, pois suas informações fraudulentas (nome, CPF, chave pix ou telefone)

estarão registradas na plataforma, a qual emitirá alertas aos usuários, quando estes consultarem o sistema.

A título de exemplo, relembrem-se os Inquéritos Policiais 183/2018, 184/2018, 313/2018, 331/2018 e 333/2018, da Polícia Civil do Estado do Amapá, os quais reuniram dezenas de boletins de ocorrência referentes ao mesmo reeducando do sistema penitenciário amapaense, o qual, apesar de estar preso, conseguia ter acesso a aparelhos celulares, por meio dos quais acessava plataformas de compra e venda online (como OLX e o *market place* do *Facebook*) e aplicava diversos golpes, nos quais se apresentava como sendo o então Diretor-Presidente do DETRAN/AP, e dizia estar interessado em itens de elevado valor econômico que estavam expostos à venda.

As vítimas, acreditando tratar-se de uma autoridade de notável confiança e prestígio social, entregavam os objetos que estavam vendendo, mediante o recebimento de um comprovante de transferência bancária falsificado.

Em todos os casos dos inquéritos acima mencionados, o estelionatário utilizava o mesmo número de telefone celular, por meio do qual conversava com as vítimas pelo aplicativo de mensageria *Whatsapp*.

Nos casos em tela, se já houvesse uma plataforma de consultas e alertas como o SARA, certamente, o infrator não teria tido tanto êxito em sua empreitada criminosa, alcançando um número de vítimas bem menor, pois, quando as pessoas verificassem no aplicativo a existência de alertas com a mesma linha telefônica, ficariam mais atentas e, possivelmente, conseguiriam evitar a consumação do crime.

6.2 – Engajamento Público e Participação Ativa da População

O sucesso do SARA também será medido pelo engajamento da população, avaliado pelo número de downloads do aplicativo, taxa de adesão e frequência de utilização.

Espera-se que a população utilize o SARA como mais uma ferramenta de verificação de segurança antes de realizar compras, transações, transferências bancárias e negociações online. Além disso, o *feedback* dos usuários, tanto em avaliações positivas quanto em sugestões de melhoria, será um indicador crucial para mensurar a aceitação e utilidade da ferramenta no cotidiano social.

Busca-se, assim, a construção de uma cultura de segurança digital, pois, com o tempo e o uso recorrente, a plataforma educará os usuários sobre a prevenção de fraudes e acerca da importância de verificar informações antes de concretizar transações por meio virtual.

Neste sentido, a fim de saber se as pessoas utilizariam a plataforma e confiariam em suas informações, realizou-se uma pesquisa por meio de preenchimento de formulário eletrônico, com questionamentos acerca da percepção das pessoas sobre o uso da plataforma e sua confiança nos alertas emitidos. Verificou-se:

- 84,9% dos entrevistados acreditam que um sistema de alertas ajudaria a prevenir fraudes;
- 74,8% disseram que confiariam nos alertas emitidos; e
- 95,4% responderam que não fariam negócio, caso recebessem o alerta de possível golpe. (pesquisa no apêndice – Anexo II)

Esses números evidenciam que o SARA apresenta alta aceitação popular e um impacto direto na prevenção de fraudes. Se a maioria dos cidadãos seguir os alertas emitidos, o número de golpes pode reduzir significativamente, criando uma nova cultura de proteção digital.

Outro ponto relevante é que 66,4% dos entrevistados afirmaram que utilizariam um sistema como o SARA para se informar sobre fraudes virtuais. Contudo, apenas 53,9% das pessoas já usam plataformas de prevenção, como Reclame Aqui e Consumidor.gov, o que indica que quase metade da população não possui ferramentas eficientes de proteção contra fraudes. Não podemos afirmar se isso acontece em razão da falta de interesse do cidadão, ou se é pela desinformação, porém, é importante asseverar que o SARA preenche essa lacuna quando fornece uma ferramenta acessível, confiável e amplamente aceita, que incentiva a população a adotar medidas preventivas contra golpes virtuais.

6.3 – Melhoria na Percepção de Segurança e Redução do Medo do Crime

A plataforma SARA fornecerá alertas anonimizados, em tempo real, acerca de golpes ativos e registrados no banco de dados da Secretaria de Segurança Pública, auxiliando a população a se sentir mais segura e também mais informada. Destarte, espera-se que o SARA impacte positivamente a sensação de segurança da população goiana. Esse impacto será avaliado por meio de pesquisas de opinião realizadas em diferentes momentos: antes da implementação do aplicativo e em intervalos regulares após seu lançamento.

Acredita-se que, com mais informações, haja uma redução da sensação de vulnerabilidade dos cidadãos, que resultará na diminuição do medo do crime digital e no aumento da confiança nas políticas públicas de segurança.

Busca-se, ainda, a atenuação dos impactos psicológicos sofridos pelas vítimas das fraudes, as quais, por vezes, sofrem com estresse, ansiedade e até depressão por conta do prejuízo sofrido. A prevenção proporcionada pelo SARA ajudará a evitar esses impactos negativos, contribuindo, também, para o bem-estar social e mental dos usuários.

6.4 – Fortalecimento da Prevenção Criminal

Ao permitir a identificação e o mapeamento de padrões de fraudes virtuais, bem como a disseminação de alertas em tempo real, a plataforma reforçará a capacidade das forças de segurança em atuar preventivamente, obstando a consumação de novos casos de fraude eletrônica. Esse impacto deverá ser refletido na maior eficiência na investigação e resolução de casos, fortalecendo a atuação policial no combate ao cibercrime.

Ademais, o sistema deverá ser atualizado constantemente, para identificar novas estratégias criminosas, bem como para implementar melhorias que facilitem o uso e a navegação por parte dos cidadãos.

6.5 – Fomento à Inovação na Segurança Pública

A implementação da plataforma SARA servirá como modelo de inovação e de boas práticas na segurança pública digital e no setor público de uma forma geral, posicionando Goiás como referência em iniciativas de segurança digital.

Os dados coletados pelo aplicativo ajudarão no desenvolvimento de novas estratégias de enfrentamento ao cibercrime e a organizações criminosas que viram no estelionato virtual campo fértil para aplicação de golpes.

6.6 – Educação Digital e Conscientização Social

Com a utilização do aplicativo, espera-se, ainda, o fomento da educação digital dos usuários, uma vez que serão realizadas campanhas educativas sobre estelionato virtual, havendo, na plataforma, uma seção exclusiva com vídeos curtos, explicativos e atualizados sobre os golpes mais comuns e dicas de prevenção.

Acredita-se que o formato visual e dinâmico garantirá maior adesão e engajamento da população no uso do sistema.

Por derradeiro, almeja-se que os usuários que acessarem os conteúdos educativos aprenderão boas práticas de segurança digital, reduzindo sua vulnerabilidade. Do mesmo modo, empresas e instituições poderão usar o SARA como ferramenta de treinamento para funcionários e clientes, sendo mais um instrumento de prevenção ao cibercrime.

7. CONCLUSÃO

O desenvolvimento do SARA deve representar um marco inovador na segurança pública, ao integrar tecnologia, inteligência e engajamento social para combater o crescente desafio dos crimes de estelionato virtual. Este trabalho busca destacar a relevância do sistema como uma ferramenta essencial para a diminuição dos dados estatísticos alarmantes e a crescente criminalidade do cibercrime, enfatizando sua capacidade de prevenir fraudes, aumentar a percepção de segurança e promover a confiança nas instituições públicas. Sem olvidar da estreita correlação com a proteção dos direitos humanos de 1ª e 5ª geração, como a vida, a saúde pública, o patrimônio, um meio virtual seguro e o bem estar social pela redução do medo do crime.

Ao longo do estudo, foram identificados desafios importantes, tanto técnicos quanto culturais. Entre os desafios técnicos, destacam-se a necessidade de garantir a robustez do sistema, proteger os dados dos usuários de forma irrestrita e assegurar a correta aplicação da lei. No âmbito cultural, a resistência inicial ao uso de novas ferramentas tecnológicas e a necessidade de conscientização da população quanto à importância da participação ativa no sistema exigem estratégias específicas de educação e comunicação.

Como recomendações para superar essas barreiras, sugere-se a realização de campanhas educativas amplas, a formação contínua dos agentes de segurança e o fortalecimento das parcerias entre o setor público e privado para garantir o aperfeiçoamento contínuo do SARA.

A urgência da implementação do sistema também é elementar predominante do presente trabalho, haja vista estar intrinsecamente relacionado com o impacto social das fraudes. Os dados da pesquisa deixam claro que o SARA não é apenas uma proposta inovadora, mas uma necessidade real e atual para a sociedade. Isso está demonstrado no alto índice de conhecimento sobre fraudes e o medo dos impactos financeiros e emocionais que assolam toda a sociedade, mostrando que o crime cibernético afeta amplamente a população.

Além do mais, a confiança no sistema e o alto índice de aceitação dos alertas, demonstrados na pesquisa, evidenciam que o SARA tem potencial para mudar o comportamento da sociedade em relação a golpes. De igual forma, a lacuna de ferramentas eficazes de proteção reforça que o SARA pode ser um divisor de águas na segurança digital, criando uma nova cultura de prevenção e garantindo mais segurança financeira e psicológica para a população.

Em termos de perspectivas futuras, o SARA tem potencial para ir além de sua implementação inicial no Estado de Goiás, expandindo para outros estados brasileiros. Associada à integração com tecnologias complementares, o SARA utiliza inteligência artificial, big data e ferramentas de monitoramento avançado, o que pode consolidar o projeto como referência nacional na prevenção de crimes digitais.

É importante destacar que um projeto dessa envergadura, embora os altos índices de benefícios que trará à segurança pública, tem uma expectativa de gastos relativamente baixos. Os principais investimentos envolverão a criação e desenvolvimento do sistema, a produção de vídeos explicativos e informativos, a atualização contínua desses conteúdos conforme novos golpes e crimes surgirem, além do aperfeiçoamento dos policiais responsáveis por alimentar e operar a plataforma. Essa capacitação garantirá que o sistema funcione de maneira eficaz e se mantenha atualizado, assegurando a máxima eficiência nas investigações e na prevenção criminal. Assim, o retorno social e a redução dos índices de criminalidade justificam amplamente os custos iniciais do projeto, que devem ser analisados de maneira pormenorizada.

Por fim, reforça-se a visão estratégica do SARA como um projeto escalável e de longo prazo, com capacidade de evoluir e adaptar-se às dinâmicas tecnológicas e criminosas. Com o avanço de sua aplicação, espera-se que o sistema contribua para a consolidação de uma cultura de segurança digital no Brasil, promovendo um ambiente mais seguro e inclusivo para todos.

8 – BIBLIOGRAFIA

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Revista de Direito da Cidade*, v. X, n. 3, p. 1234-1256, 2018. Disponível em: https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/?format=pdf&lang=pt . Acesso em: 24 jan. 2025.

BRASIL. Decreto lei nº 2.848 de 07 de dezembro de 1940, Código Penal, Brasília, DF, Presidência da República. [2019]. Disponível: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm . Acesso em: 23 de janeiro de 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 05 de outubro de 1988. Brasília, DF: Assembleia Constituinte, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm . Acesso em: 23 de janeiro abr. 2025.

BRASIL. Lei n.º 12.737 de 30 de novembro de 2012 – DF, Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm . Acesso em 23 de janeiro de 2025.

BRASIL. Lei n.º 13.709 de 14 de agosto de 2018 – LEI DE GARANTIAS E PROTEÇÃO DE DADOS - LGPD, DF, Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em 23 de janeiro de 2025.

BRASIL. Emenda Constitucional 115 de 22 de fevereiro de 2022 – DF, Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm . Acesso em 24 de janeiro de 2025.

BRASIL. Lei n.º 14.478 de 21 de dezembro de 2022 – DF, Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm . Acesso em 23 de janeiro de 2025.

CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático, 2003.

Declaração Universal dos Direitos Humanos. Assembleia Geral das Nações Unidas, 1948. Disponível em: http://www.un.org/pt/universal-declaration-human-rights/. Acesso em: 23 jan. 2025.

DICKSON, Carvalho Gonçalves da Silva. CRIMES CIBERNÉTICOS: LIMITES E DESAFIOS DA INVESTIGAÇÃO. Disponível em http://repositorio.undb.edu.br/bitstream/areas/834/1/DICKSON%20CARVALHO%20GONCALVES%20DA%20SILVA.pdf acesso em

TEYMISSO, SEBASTIAN FERNANDES MAIA. ANÁLISE DOS MECANISMOS DE COMBATE AOS CRIMES CIBERNÉTICOS NO SISTEMA PENAL BRASILEIRO - disponível em https://repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf

O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet. Felipe Ferreira Diniz1Jacqueline Ribeiro Cardoso2Eduardo Henrique Pompeu Puglia3. Disponível em https://www.periodicos.famig.edu.br/index.php/direito/article/view/215/142

CRIME DE ESTELIONATO VIRTUAL COMO FATOR DE VIOLAÇÃO À HONRA DA PESSOA CRIME OF VIRTUAL ESTELIONATO AS A FATOR OF VIOLAÇÃO À HONRA DA PESSOA DELITO DE VAPOR VIRTUAL COMO FACTOR DE VIOLACIÓN AL HONOR Lara Beatriz Martins Pimenta de Siqueira. Diolina Rodrigues Santiago Silva. Disponível em https://periodicorease.pro.br/rease/article/view/11531/5168

LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas, SP: Ed. Millennium, 2005,

MIRANDA, Zil. Política de ciência, tecnologia e inovação para segurança pública. Revista Brasileira de Segurança Pública, v. 6, p. 434-453, 2012.

VAZ, Paulo Afonso Brum**. Tutelas de urgência e o princípio da fungibilidade**: § 7º, do art. 273 do CPC. *Revista de Processo*, São Paulo, v. 32, n. 144, p. 23-37, fev. 2002.

Brown, L., & Martinez, R. (2022). Crime reporting and police controlling: Mobile and web-based approach for information-sharing in Iraq. *Journal of Mobile Applications, 18*(2), 123-137.

Galila, G. B. (2023). Crimeline: Empowering public safety with GIS-based crime incident reporting. *International Journal of Advanced Research in Science, Communication and Technology, 3*(2), 787-792. https://doi.org/10.48175/IJARSCT-12309

Nguyen, T., & Williams, B. (2022). Development of a software system for real-time management of crime reports in southwestern Nigeria: The administrative approach. *Journal of Crime Science, 22*(6), 401-415.

Smith, J., & Johnson, M. (2023). Leveraging big data analytics to combat emerging financial fraud schemes in the USA. *International Journal of Crime Prevention, 28*(4), 401-415.

SARA

Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Login

Senha

Não tenho conta

Esqueci a senha

ENTRAR

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO

SECRETARIA DE ESTADO
DA SEGURANÇA PÚBLICA

SARA

Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Nome

CPF

Data de Nascimento

Senha

Confirmar Senha

Concordo com o **TERMO DE USO**

CADASTRAR

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO

SECRETARIA DE ESTADO
DA SEGURANÇA PÚBLICA

SARA

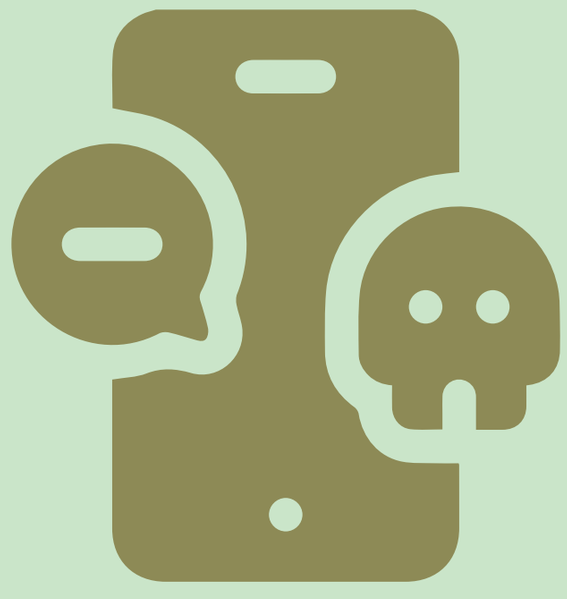
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

ESTÁ COM DÚVIDA?

FAÇA UMA **PESQUISA**

FUI VÍTIMA **DE GOLPE**

O QUE FAZER?



ORIENTE-SE

GOLPES MAIS **APLICADOS**

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO

SECRETARIA DE ESTADO
DA SEGURANÇA PÚBLICA

Olá, **Rackell Oliveira**

- **Perfil** *(complete seu perfil)*
- **FAÇA UMA PESQUISA**
- **Como Funciona?**
- **Termos de Uso**
- **Uso de Dados Pessoais**
- **Quem Somos?**
- **Segurança**
- **Sair**

V. 1.0.2

ARA

e Alerta Referencial Anonimizado
stelionato e outras fraudes

VIDA?
MA
ISA

MA
PE
R?

MAIS
OOS

SECRETARIA DE ESTADO
DA SEGURANÇA PÚBLICA

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Meu **Perfil**

Adicionar Foto

Rackell Marques de Oliveira

Nível Conta: Ouro

Nome Completo

Rackell Marques de Oliveira

CPF

986.*.***-20**

Data de Nascimento

18/04/1983

Celular

(64) 99999-9999

E-mail

loremipsum@provedor.com.br

Logradouro

Av. Lorem Ipsum

Complemento

Qd. 20, Lt 3

Bairro

Centro

CEP

76.105-000

Cidade

Firminópolis

Estado

GO

País

BR

ATUALIZAR

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Faça uma **Busca**

Pesquisar **EMPRESA** por nome ou **CNPJ**

Pesquisar **PESSOA FÍSICA** por **CPF**

Pesquisar **CHAVE PIX** ou **CONTA BANCÁRIA**

Pesquisar **TELEFONE**

Pesquisar **SITES**

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Faça uma **Busca**

Empresa de Eletrônico LTDA

A sua busca
Minha Empresa LTDA
retornou
0
ocorrências policiais

continue a transação observando os cuidados necessários

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Faça uma **Busca**

Pesquisar **EMPRESA** por nome ou **CNPJ**

A sua busca
123.456.789-00
retornou
5
ocorrências policiais

possível golpe, tome maiores cuidados

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO
SECRETARIA DE ESTADO
DA SEGURANÇA PÚBLICA

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Faça uma **Busca**

Pesquisar **EMPRESA** por nome ou **CNPJ**

A sua busca
Ag: 0000 CC: 0001111-1
retornou
10
ocorrências policiais

possível golpe, não realize transações sem auxílio de autoridade

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

SARA
Sistema de Alerta Referencial Anonimizado
Estelionato e outras fraudes

Faça uma **Busca**

Pesquisar **EMPRESA** por nome ou **CNPJ**

A sua busca
www.meusite.com.br
retornou
11
ocorrências policiais

possível golpe, perigo concreto na transação.
Você pode ser a próxima vítima

GOVERNO DE GOIÁS
O ESTADO QUE DÁ CERTO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

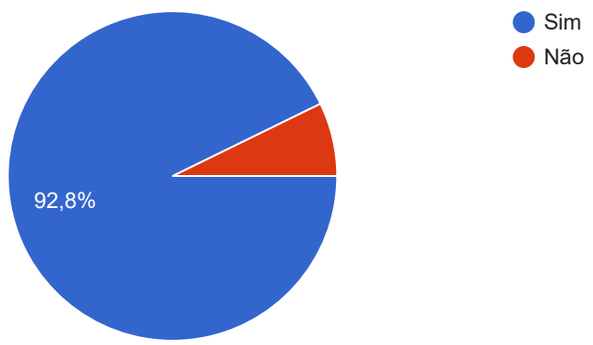
Pesquisa SARA - Sistema de Alerta Referencial Anonimizado

152 respostas

Você tem conhecimento sobre casos de fraudes eletrônicas?

Copiar

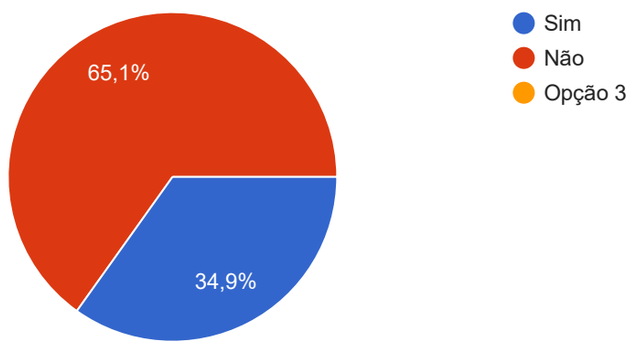
152 respostas



Você já foi vítima de estelionato?

Copiar

152 respostas



Se sim, quais foram os impactos mais significativos do crime para você (financeiros, emocionais, sociais, etc.)?

152 respostas

Não

Financeiro

Financeiros

Não fui vítima

Financeiro

Nao

Financeiro e emocional

Nunca fui vítima

Todos

.

Nenhum

Não fui vítima

Não fui vítima de estelionato

-

.

Prejudicado

Emocionais

Nunca fui

Financeiros

Financeiro e emocional.

Emocionais

Não fui vítima de estelionato.

não

Não

Sentimento de lesado.

NA

Financeiro e emocional.

(não foi eletrônico)Tive uma perda financeira de 13 mil, um abalo emocional por muitos tempo, ainda mais sabendo que esse tipo de crime os estelionatário ficam pouco tempo na cadeia se condenado e quando preso pode pagar fiança.

Nao tive

,

Financeiro. Perdemos uma quantia em dinheiro

Nao fui vítima, mas o impacto do golpe é mais emocional, muitos não queixam dos golpes por terem vergonha de falar que foi vítima de golpe (ainda mais se tratando de golpe cibernético).

Financeiros, emocionais, sociais, todos possíveis

Nunca fui vítima.

Não fiz, transferência bancária

Emocionais: medo e insegurança.

Não!

Não fui

Impacto financeiro e emocional

Financeiros
No

Prejudicada

Nunca aconteceu comigo, mas já aconteceu com minha mãe

não

Não fui vítima , graças a Deus 🙏

Não sofri, pois percebi a tempo que se tratava de um golpe.

Não. Só uma tentativa do cartão mais não prossegui com o pedido.

não fui

Não passei por isso, mas quem passa o impacto mais evidente e o financeiro e emocional.

Financeiros e emocionais, principalmente para idosos.

Não chegou ser financeiro porque caímos na real antes.

emocionais, fiquei com vergonha

Não fui vítima, mas conheço quem foi. Impactos financeiros e emocionais.

Não fui

Nunca fui vítima de estelionato

Socialmente é um abalo muito forte perante a sociedade, pois sempre atinge as pessoas mais vulneráveis.

Emocionais ,financeira

Financeiro, mas principalmente emocional. Muito ruim se sentir impotente e enganada

Nunca cai, mas já ouvi muitas pessoas falarem sobre a perda financeira e como se sentem mal psicologicamente.

Não se aplica

Ambos

Todos

Socias

não tive impacto significativo porque prendi a envolvida antes do prejuízo.

Não sofri nenhum caso

Emocionais.

Nao fui vitima

Nunca passei por essa situação

Não teve

Financeiros e emocionais

Nunca fui vítima de estelionato.

Emocionais, visto que a fraude foi coberta pela instituição financeira, mas gerou transtornos emocionais, visto que tive de perder um bom tempo para recuperar os valores.

Nunca sofri golpe por meio eletrônico, mas acredito que além do prejuízo financeiro, há um grande impacto negativo na parte emocional da vítima. Como realizará outras transações financeiras sem se preocupar?

Não fui vítima por ter percebido que poderia ser golpe

Riscos financeiros

Prejudicado

Não se aplica

Emocionais e Sociais

Financeiros, emocionais.

Houve tentativa, porém, não concluída.

Financeiros.

Sofri apenas tentativas... várias...

Golpe do pix

Não passei por essa experiência!

Pedi uma quantia significativa, e não sei como fazer o BO

Nao fui vítima

Acredito que financeiros e emocionais dependendo do caso.

Emocional e social

Social e emocional

NÃO

Emocional e financeiro

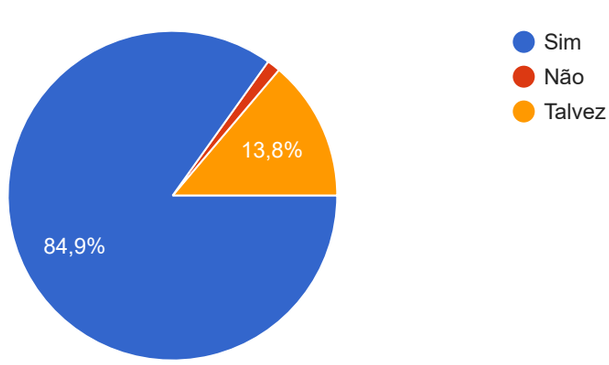
Emocional

Emocionais e financeiros

Em sua percepção, um sistema de alertas para advertir e orientar o cidadão acerca de criminosos, com dados como nomes, CPF/CNPJ e/ou chaves pix, seria útil para prevenir novos casos de estelionato?

Copiar

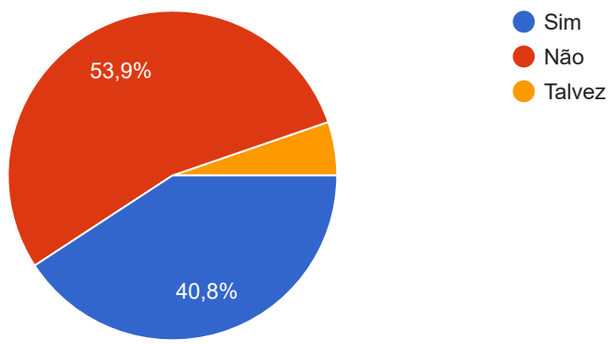
152 respostas



Você já utiliza alguma plataforma digital para se prevenir de fraudes eletrônicas (como o Reclame Aqui ou Consumidor.gov)?

Copiar

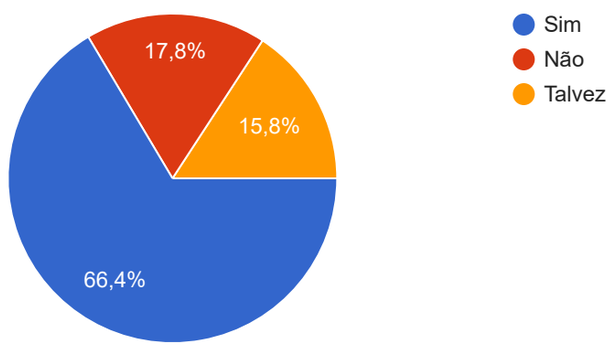
152 respostas



Você utilizaria um aplicativo como o SARA para se informar sobre fraudes virtuais?

Copiar

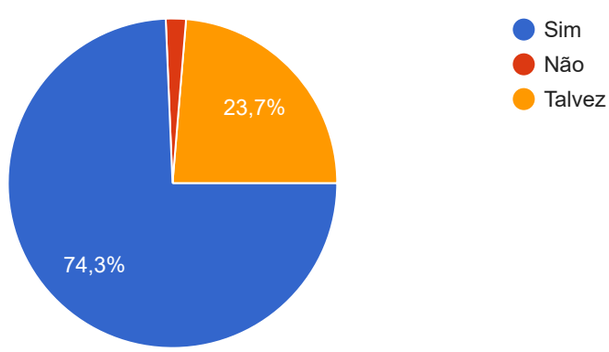
152 respostas



Você confiaria em alertas emitidos pelo SARA?

Copiar

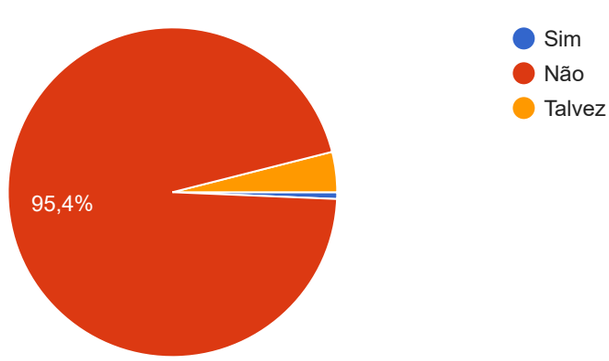
152 respostas



Se você recebesse alerta de possível golpe, ainda assim, faria negócio?

Copiar

152 respostas



Copiar

Você acredita que o SARA poderia ajudar a reduzir os casos de estelionato virtual?

152 respostas