Especificação e Implementação de uma Plataforma para Compartilhamento de Dados de Investigações e Perícias: Uma Abordagem Centrada na Inteligência Cibernética

Giulia Chiucchi Silva[1], João Benedito dos Santos Junior[1]

[1]Instituto de Ciências Exatas e Informática – ICEI
Pontifícia Universidade Católica de Minas Gerais – PUC Minas
Belo Horizonte – MG – Brasil

giulia.chiucchi@sga.pucminas.br, joao@pucpcaldas.br

Abstract. *Public safety is fundamental to the well-being of society and technology plays an important role in this respect. During the investigation of the most varied types of crimes and in the expert examination phase, evidence, specially that in digital way, is collected and stored by security agents and investigators. Multiple organizational and operational structures can be observed in the most varied departments of the Security and Law Forces, not always adequate for the daily activities of fighting crime. In this context, it becomes relevant to specify and implement a computational solution, proposed in this work, that presents a software platform, in the Web environment, that allows the recording and storage of the collected evidence, as well as the application of intelligence filters to offer sharing services between investigators and security officers, as well as between investigations.*

Keywords *– Web Platform, Cyber Threat Intelligence, Forensics Investigations.*

Resumo. *A segurança pública é fundamental para o bem-estar da sociedade e a tecnologia tem um papel importante nesse aspecto. Durante a investigação dos mais variados tipos de crimes e na fase de exames periciais, evidências, especialmente aquelas em formato digital, são coletadas e armazenadas por agentes de segurança e investigadores. Múltiplas estruturas organizacionais e operacionais podem ser observadas nos mais variados departamentos das Forças de Segurança e Lei, nem sempre adequadas para as atividades cotidianas de combate à criminalidade. Neste contexto, torna-se relevante especificar e implementar uma solução computacional, proposta neste trabalho, que apresente uma plataforma de software, no ambiente da Web, que permita o registro e o armazenamento das evidências coletadas, bem como a aplicação de filtros de inteligência para oferecer serviços de compartilhamento entre investigadores e agentes de segurança, bem como entre investigações.*

Palavras-chave *– Plataforma Web, Inteligência, Perícia e Investigação.*

1. Introdução

Atualmente, redes de comunicação em escala global, como é o caso da Internet, estão disponíveis para uso pela sociedade, das mais diversas formas, atingindo cerca de 82,9% dos lares brasileiros (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br, 2020), sendo que que cada cidadão brasileiro possui, em média,

3,6 dispositivos conectados, produzindo cerca de 1,5GB de dados diariamente. De um modo geral, a utilização das redes de comunicação pode resultar em benefícios ao cidadão, mas também pode ser direcionada para a criminalidade, em suas mais variadas formas e tipificações. No contexto da investigação de crimes e na realização de exames periciais, um significativo volume de dados e informações pode ser coletado e/ou gerado por ações dos investigadores e peritos. Deve-se considerar que uma parte desses dados e informações pode guardar relação com outras investigações e perícias já realizadas e/ou em andamento. Neste contexto, este trabalho pretende oferecer uma solução computacional, na forma de uma plataforma de software via web, que seja, portanto, acessível de qualquer lugar e a qualquer momento, que permita o registro, o armazenamento e o estabelecimento de correlações entre evidências digitais coletadas.

Este trabalho está organizado em 5 (cinco) seções. A **seção 2** aborda o estado da arte no contexto em que este trabalho está inserido, listando trabalhos relacionados ao tema central desta proposta; na **seção 3**, são apresentados os aspectos essenciais da Inteligência Cibernética; na **seção 4**, a metodologia para solução do problema é apresentada, descrevendo os detalhes da especificação e da implementação da plataforma; a **seção 5** apresenta o planejamento dos experimentos e os resultados preliminares obtidos; por fim, a **seção 6** apresenta as considerações finais e os trabalhos futuros.

2. Contextualização e Referencial Teórico

No Brasil, a esfera da segurança pública se divide entre diferentes institutos, tendo uma abrangência nacional. Na estrutura organizacional, órgãos especializados são instituídos para a realização de tarefas específicas, como é o caso do suporte e competência técnica para as atividades de investigação e perícia, no âmbito da segurança pública. Entre esses órgãos especializados, destacam-se as polícias científicas e órgãos de inteligência, como é o caso da Agência Brasileira de Inteligência (ABIN).

O processo de resolução de casos criminais envolve uma série de etapas, que podem variar a cada caso, mas que, geralmente, são as seguintes: a) a ocorrência de um crime é notificada e registrada em um boletim formal (boletim de ocorrência); b) com as principais informações reunidas, a fase de inquérito é iniciada, sendo iniciada a investigação, conduzida por agentes de Segurança e Lei, etapa em que ocorre a coleta e análise de dados, na forma de evidências, que poderão se tornar provas com validade em um Tribunal de Justiça; c) após a etapa de inquérito, com base nas provas e nos indícios, o Ministério Público oferece a denúncia ou a queixa-crime contra o(s) autor(es) do crime, iniciando a fase de persecução penal, em que o Poder Judiciário analisa o caso e profere a sentença, que pode ser de condenação ou de absolvição. A sentença encerra o caso, salvo se houver recurso das partes.

A proposta de plataforma de software, apresentada neste trabalho, está centrada na etapa de inquérito policial, servindo com ferramenta para o registro e o armazenamento das evidências coletadas na investigação e/ou perícia, e provendo informações que permitam o cruzamento dessas evidências com outros inquéritos e perícias já realizados e/ou em andamento. Este trabalho não tem vínculos com o sistema de registro dos boletins de ocorrência, uma vez que os sistemas para essa finalidade são específicos da Polícia Militar de cada estado da federação, que não tem a competência para as atividades de investigação e perícia.

(MCGARRELL; FREILICH; CHERMAK, 2007) apresentam em sua pesquisa uma importante iniciativa para reduzir o crime armado, o PSN (*Project Safe Neighborhoods*), modelo que envolve forças variadas que trabalham de forma estratégica utilizando análise de padrões criminais para desenvolvimento de suas estratégias e compartilhamento de informações valiosas para as operações. Após a revisão de casos que obtiveram êxito ao utilizar da iniciativa de coleta de informações de diferentes fontes e compartilhamento entre forças diferentes, foi concluído e definido a necessidade de ter níveis amplos e equilibrados de análise perspicaz e estratégica das ameaças e da inteligência tática específica em indivíduos e grupos, de forma descentralizada e compartilhada.

Como complemento à proposta anterior, (MACHINA; SONGJIANG, 2020) apresentaram em sua obra a investigação nas bases policiais da Nigéria em busca de um modelo que pudesse analisar um grande volume de dados e compartilhar entre as instituições, para melhorar as ações de combate ao crime. Em síntese, o sistema funciona com a autenticação do usuário e oferece a opção de adicionar uma informação, que é verificada nos bancos de dados de crimes já registrados; o sistema, então, oferece relatórios para usuários de diversos níveis dentro da hierarquia da organização de segurança e lei.

A mesma preocupação referente à análise de dados policiais foi apontada na publicação de (CHERMAK et al., 2013), ao tratar o assunto como uma necessidade de cooperação nacional, defendendo como elemento chave a ampla distribuição de informações para o êxito no seu uso para a prevenção de ataques, sendo a relação entre os responsáveis pela aplicação da lei e as outras organizações um ponto crítico para o sucesso no compartilhamento. Foi discutido o desafio de se obter e administrar dados considerados relevantes mesmo que a tecnologia tenha possibilitado a coleta e compartilhamento de *big data* de uma forma mais fácil. O problema relatado é abordado na revisão de (TREGLIA; PARK, 2009), introduzindo um método possível de observar os efeitos resultantes de ajustes nas diferentes áreas de influência segundo o nível de compartilhamento de informações. A partir disso, foi confirmada a teoria de que a cooperação entre as forças policiais é afetada diretamente pelos fatores técnico, social e legal. Utilizando o método e a teoria como base é possível avaliar e reconhecer os fatores principais e o seu impacto no sistema para soluções serem identificadas e por fim implementadas.

A colaboração é vista como um ponto-chave na investigação de crimes; (KANCA, 2021) avaliaram a necessidade do compartilhamento em um cenário empresarial sobre ameaças cibernéticas. Os pesquisadores utilizaram a análise de lacunas de informação de Zack, que detalha como uma organização pode alcançar um equilíbrio entre o que pode ser feito e o que necessariamente será viabilizado para decidir o que é considerado indispensável sobre as informações das ameaças para o aperfeiçoamento da defesa em organizações, determinando por fim o mecanismo de cooperação para obter esse equilíbrio, prevendo a expansão da coleta, armazenamento, distribuição e compartilhamento de informações entre organizações. (CAI D. LI, 2020) trabalha em um outro panorama acerca do uso de *big data* na prevenção de crimes, desenvolvendo um sistema baseado em dispositivos IOT geradores de imagens em um contexto industrial. Além de apresentar a composição do sistema embutido de visão computacional, houve uma discussão a respeito da necessidade da aplicação da teoria de governança multicêntrica, conceito em que diferentes agentes governamentais possam realizar o processo de administração,

cooperando entre si, fornecendo informações para abastecer sistemas de inteligência policial.

O conceito de *data mining* foi o preposto para a análise do grande volume de dados, (SEIDLER, 2013) aborda o conceito como forma de automatizar a metodologia de trabalho dos peritos criminais em conjunto com o Modelo de Inteligência Nacional (estrutura de trabalho aplicada em algumas forças policiais pelo mundo). A abordagem aplica o padrão CRISP-DM (*Cross Industry Standard Process for Data Mining*), adaptando aos desafios de uma análise no âmbito criminal. O sistema utiliza-se desse padrão para a criação do modelo e a manutenção garante que os dados resultantes estarão sempre atualizados e disponíveis para os agentes de segurança e lei, que atuam diretamente nas ações de investigação.

No desenvolvimento do framework de análise e compartilhamento de informações policiais de (PRAMANIK RAYMOND Y. K. LAU, 2017), mecanismos de *data mining* foram utilizados na etapa de análise dos dados, testando diferentes formas antes da escolha do SNA (*Social Network Analysis*), resultando em métodos que permitem o agrupamento de dados, a associação entre pessoa e eventos e a extração de padrões dessas relações. (ADEDAYO, 2016) apresentou o conceito de um *framework* que tem como objetivo o auxílio de peritos em todas as etapas do processo de análise dos dados em investigações. O *framework* separa o procedimento de investigação forense digital em sete passos distintos, com uso de múltiplas ferramentas computacionais, contemplando as etapas de triagem, redução de dados em *subsets*, análise de agrupamento, *data mining*, computação distribuída e análise inteligente.

3. Aspectos Essenciais da Inteligência Cibernética

Entende-se por Inteligência Cibernética como sendo um conjunto de procedimentos, ferramentas (tecnológicas ou não), mecanismos e ações para tratar a ocorrência de ataques, incidentes, eventos e crimes de natureza cibernética, que tenham um equipamento computacional como alvo (crimes próprios) ou como meio (crimes impróprios). Considerando o aspecto global e de forte conectividade, que caracteriza o Mundo Digital e o Espaço Cibernético (MARCO CIVIL DA INTERNET, 2014), cabe destacar que existem muitos tipos de ataques, incidentes, eventos e crimes que podem estar relacionados, de alguma forma, com a coleta de evidências digitais em cenas de crime e nos procedimentos característicos dos exames periciais.

Segundo dados estatísticos de sistemas que monitoram o Espaço Cibernético, tais como SaferNet (https://new.safernet.org.br/), Kaspersky (https://cybermap.kaspersky.com/) e DCiber (https://dciber.org/mapas-de-ameacas/), o Brasil, em 2022, foi o terceiro país que mais sofreu ataques cibernéticos, das mais diversas naturezas e com as mais diversas finalidades (SAFERNET, 2022; HPE, 2022). Pode-se afirmar que as tecnologias são imprescindíveis para as operações do cotidiano no ambiente interno das mais variadas organizações e empresas, ao mesmo tempo que representam riscos, quando mal utilizadas (MAYER, 2013).

Neste contexto, uma plataforma para armazenar evidências coletas em investigações e perícias, bem como aplicar regras de relacionamento entre esses evidências, tanto aquelas de natureza tipicamente cibernética, quanto aquelas resultantes de articulações criminosas no ambiente cibernético e executadas no ambiente real (fora do mundo digital). Do ponto

de vista prático, a plataforma deve considerar, em suas funcionalidades, as premissas advindas do universo da Investigação e Perícia, a saber: a) MATERIALIDADE, que é comprovação física e indispensável dos vestígios deixados por um ataque, incidente, evento ou crime; b) DINÂMICA, que é a comprovação de como ocorreu um ataque, incidente, evento ou crime, que deixou vestígios (materialidade); c) AUTORIA, que é a identificação e comprovação do(s) autor(es) de um ataque, incidente, evento ou crime.

No contexto dos Sistemas de Informação, dados são elementos brutos e/ou aleatórios, que constituem a matéria-prima para produção da informação, que pode ser vista como resultado da organização, estruturação e classificação de dados. Por fim, o conhecimento ocorre quando a informação é processada e transformada em experiência para um indivíduo, grupo de indivíduos ou sociedade (CASEY, 2017).

4. A Especificação e Implementação da Plataforma

Neste trabalho, os investigadores e peritos são considerados os principais usuários da plataforma proposta; no entanto, a base de dados pode ser compartilhada com toda e qualquer autoridade policial, através de procedimentos de exportação de dados, previsto na especificação aqui reportada. De modo geral, a plataforma proposta consiste em um sistema colaborativo, que tem a capacidade de registrar, armazenar e relacionar evidências coletadas durante a investigação e exames periciais. Neste contexto, a **Tabela 01** apresenta os requisitos formais do sistema, com destaque para o seu funcionamento, o desempenho previsto e as funcionalidades essenciais.

Tabela 01 – Requisitos formais especificados para a plataforma

Requisito	Descrição
R01	O sistema deve possuir um mecanismo de autenticação forte baseado no e-mail institucional do agente de segurança e lei, com verificação do domínio a que pertence
R02	O sistema deve permitir o cadastro, edição e exclusão de investigações e perícias
R03	O sistema deve permitir a classificação e seleção de marcadores de evidências nas investigações e perícias
R04	O sistema deve enviar notificações ao identificar relações entre uma investigação corrente e outras investigações disponíveis
R05	O sistema deve disponibilizar uma listagem dos dados cadastrados
R06	O sistema deve permitir a solicitação de acesso a investigações privadas que foram identificadas como correlatas a outro usuário
R07	O sistema deve permitir a resposta referente a solicitações de acesso a investigações privadas
R08	O sistema deve permitir a visualização detalhada de investigações que possam interessar a outros usuários se públicas ou privadas, desde que o usuário tenha acesso

A partir dos requisitos formais do sistema, um modelo de diagrama de caso de uso foi utilizado para descrever e identificar os atores envolvidos e suas relações com as funcionalidades previstas para a plataforma, oferecendo uma representação visual para compreender como diferentes partes interagem e se relacionam, permitindo uma análise do sistema como um todo, como mostra a **Figura 01**.

Figura 01 – Caso de uso geral da plataforma

A partir dos requisitos formais e do modelo de caso de uso, a implementação da plataforma foi desenvolvida com um conjunto de tecnologias para o ambiente da Web, notadamente com o *framework* React, baseado na linguagem Javascript. O gerenciamento dos usuários, das investigações e o processamento dos dados foi implementado com tecnologia NodeJs, em conjunto com o *framework* Express e a linguagem Typescript. O armazenamento dos dados é realizado na infraestrutura de um banco de dados relacional, como é o caso do PostgreSQL. A **Figura 02** apresenta a síntese da arquitetura de software proposta para a plataforma.

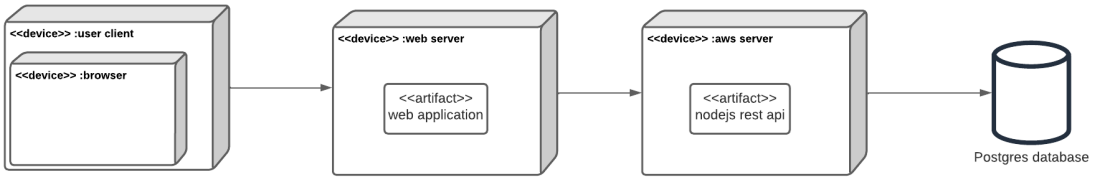

Figura 2. Esquema de implementação da aplicação

No caso do banco de dados, uma modelagem preliminar foi realizada, resultando na identificação de duas tabelas principais, que são aquelas para armazenar os **`usuários`**

e as **`investigações`** a eles relacionadas. Essas tabelas estão relacionadas de forma que um usuário pode ter várias investigações (1:n) e cada investigação está associada a apenas um usuário (1:1), através de uma chave estrangeira, como mostra a **Figura 03**.

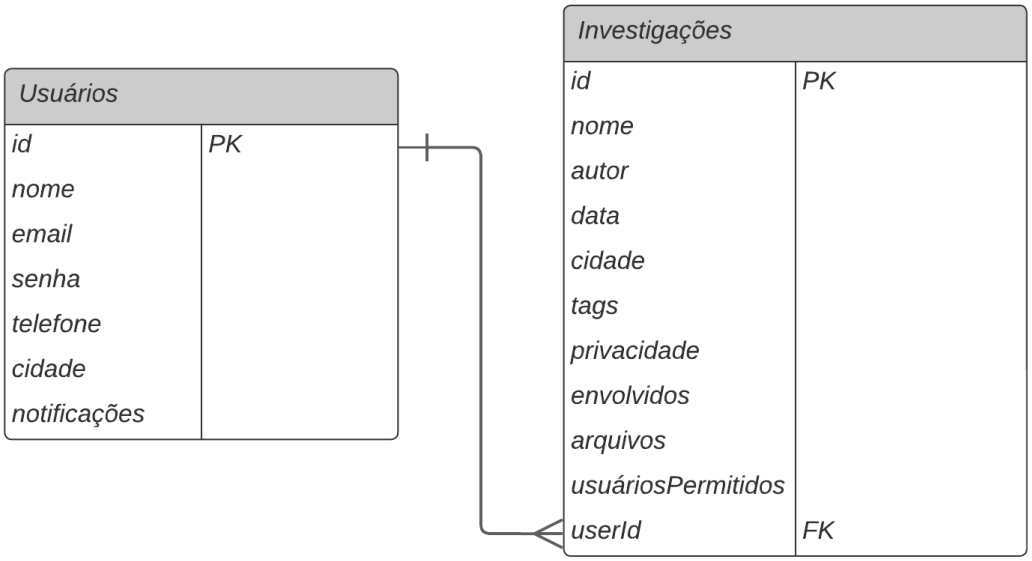

Figura 03. Diagrama entidade-relacionamento

É possível notar a existência de um atributo de investigação denominado **`privacidade`**, que permite a uma investigação ser colocada em um estado diferenciado de sensibilidade, por algum motivo específico e determinado pelo usuário que lhe deu origem, evitando que seja listada para todos os usuários da plataforma. Para integração da interface do usuário (*front-end*) com a infraestrutura de banco de dados (*back-end*), foi estabelecido um conjunto de fluxos de usabilidade, notadamente centrado nas entidades `users` e `investigations`, conforme mostram as **Tabelas 02** e **03**.

Tabela 02. *Endpoints* de *'users'*

Método	URI	Ação
`POST`	/users/create	Criar
`GET`	/users/{:id}	Exibir detalhes
`PATCH`	/users/{:id}	Editar
`DELETE`	/users/{:id}	Deletar
`POST`	/users/login	Login

Tabela 03. *Endpoints* de *'investigations'*

Método	URI	Ação
`POST`	/investigations/create	Criar
`GET`	/investigations/{:id}	Exibir detalhes
`PATCH`	/investigations/{:id}	Editar
`DELETE`	/investigations/{:id}	Deletar
`GET`	/investigations	Listar públicas

Os fluxos de usabilidade são essencialmente aqueles típicos de operações com sistemas de bancos de dados, tais como criação, listagem, atualização, exclusão e detalhamento de informações. No caso da implementação, recursos da API REST foram aplicados para garantir que os fluxos estejam adequados aos algoritmos que devem analisar as relações entre os dados oriundos das investigações e perícias, resultando em notificações que sejam efetivas para os usuários da plataforma. Para a interação entre as tabelas criadas do banco de dados, funções específicas são executadas, sempre que uma requisição ocorrer em algum dos *endpoints*. Os métodos estão localizados nos módulos controladores (*controllers*), associadas à sua respectiva entidade, conforme mostra a **Figura 04**.

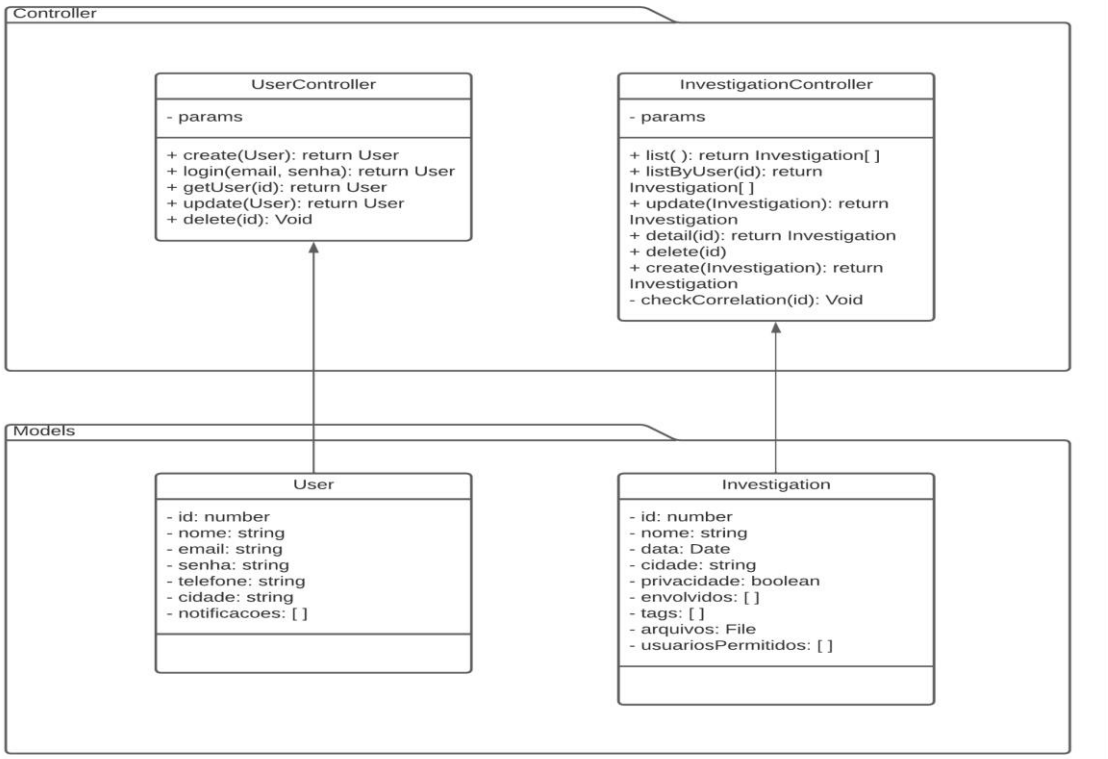

Figura 04. Diagrama de classes

Para finalizar a implementação da plataforma, os fluxos de atividade foram verificados, para que a etapa de testes pudesse ser planejada. Observou-se que a plataforma desenvolvida contempla todos os requisitos formais especificados, desde a etapa de autenticação do usuário, passando pelas funcionalidades clássicas de um sistema de banco de dados, com fechamento nas funcionalidades para relacionamento entre as evidências coletadas em investigações e perícias, além da geração de relatórios e emissão de notificações aos usuários. A **Figura 05** apresenta a visão geral da plataforma, através de um diagrama de atividade.

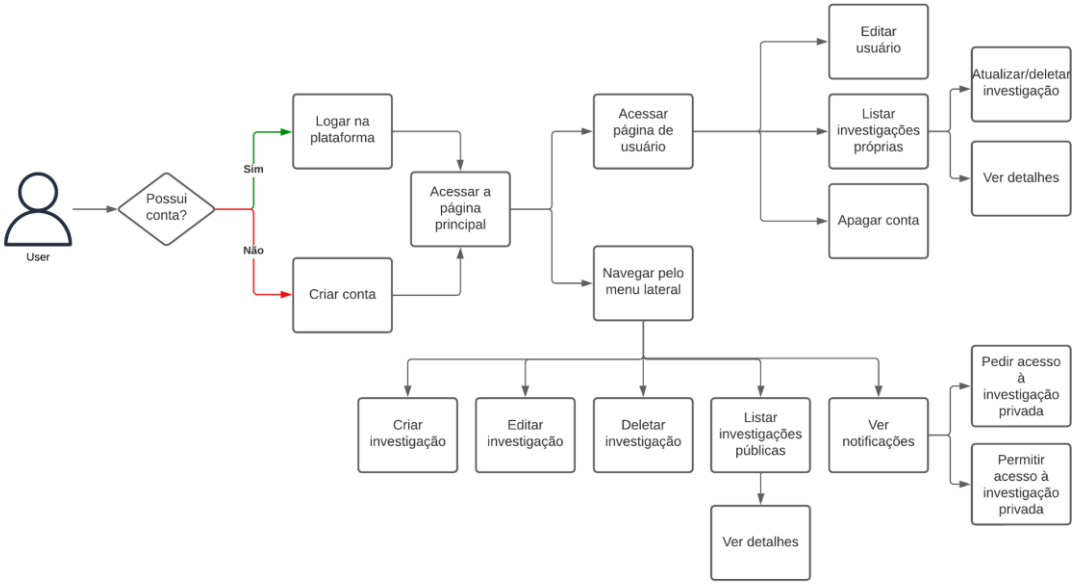

Figura 05. Fluxo das atividades típicas na plataforma

5. Testes e Resultados Preliminares

Num primeiro momento, os testes de usabilidade da plataforma foram realizados pelo orientador deste trabalho, que é Perito do Tribunal de Justiça de Minas Gerais (TJMG), do Tribunal de Justiça de São Paulo (TJSP), do Tribunal da Justiça do Trabalho (TRT), do Tribunal da Justiça Federal (JF), Perito *Ad-Hoc* das Forças de Segurança e Lei, em nível estadual e federal, além de Colaborador *Ad-Hoc* em ações específicas de alguns Ministérios Públicos Estaduais; com sua atuação em Investigação e Perícia Forense Computacional, desde 2007, o orientador deste trabalho, ao realizar os testes mínimos de usabilidade, comprovou a eficácia dos fluxos da plataforma nas operações de registro e armazenamento das evidências coletadas numa investigação e/ou perícia, mas alertou sobre a necessidade de avanços nos sistemas de notificação ao usuário. De forma complementar, os algoritmos para estabelecimento de vínculos e relacionamentos entre as evidências coletadas e entre as investigações criadas na plataforma atendem, satisfatoriamente, os requisitos formais especificados, mas podem ser evoluídos para produzir resultados surpreendentes à luz da Inteligência Cibernética, provavelmente com uso de ferramentas, técnicas e algoritmos de Inteligência Artificial, notadamente aqueles inspirados no Aprendizado de Máquina (*Machine Learning*). As **Figuras 06**, **07** e **08** apresentam *screenshots* de algumas das principais funcionalidades da plataforma.

Figura 05. Tela de listagem pública

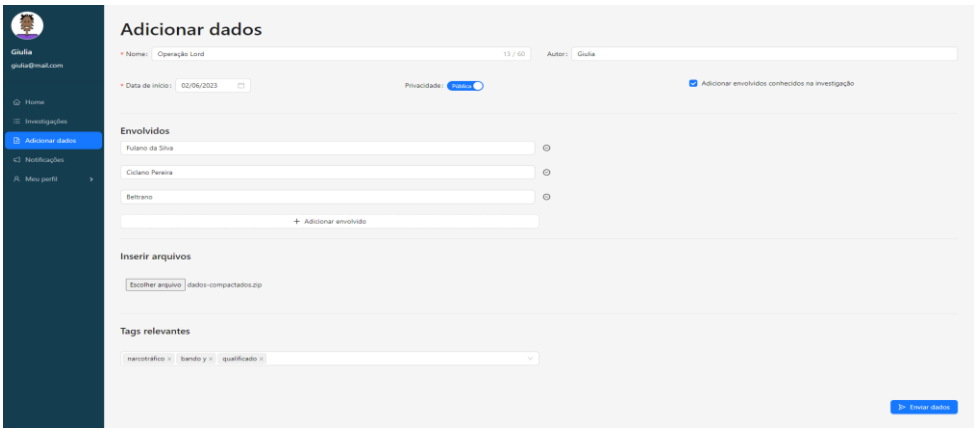

Figura 07. Adição de dados

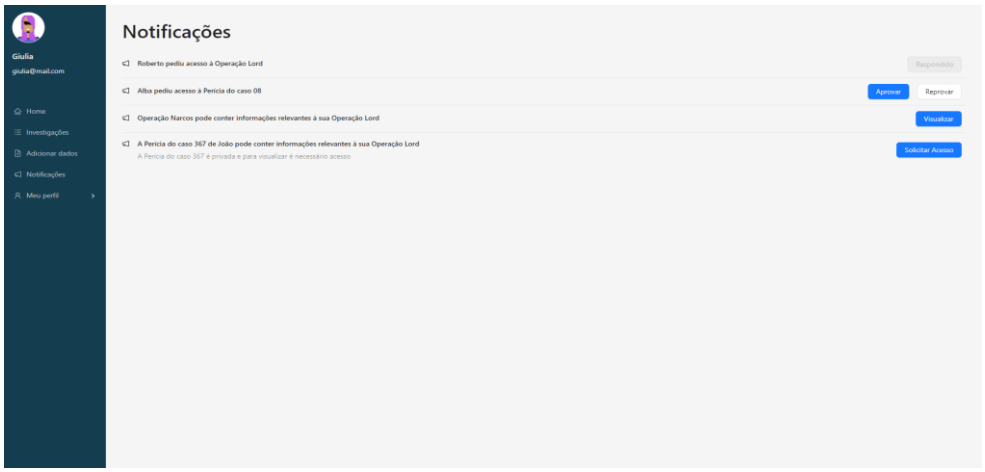

Figura 08. Notificações do usuário

Observa-se que a plataforma permite a criação de investigações e perícias (**Figura 06**), com registro dos dados que as identifiquem sumariamente. Neste ponto, é possível obter

a listagem de todas as investigações e perícias registradas, bem como detalhar as informações a elas relacionadas (**Figura 07**); operações de edição estão disponíveis em todos os níveis de visualização. Por fim, sempre que houver relacionamento e/ou vínculo entre evidências ou investigações/perícias, notificações serão emitidas e enviadas ao(s) usuário(s) que tenha(m) autorização para visualizá-las (**Figura 08**).

Num segundo momento, uma outra etapa de testes de usabilidade está prevista, envolvendo um grupo de 10 (dez) agentes de segurança e lei da Polícia Civil de Minas Gerais, no contexto da parceria já existente entre a sua Regional de Poços de Caldas e PUC Minas, *campus* Poços de Caldas. Os resultados dessa nova etapa de testes serão reportados em artigo técnico-científico.

Testes isolados também podem ser realizados, uma vez que a plataforma se encontra disponível *online* para acesso em https://intelishare.vercel.app/.

6. Considerações Finais e Trabalhos Futuros

Conforme descrito, os testes foram realizados em ambiente controlado e os resultados obtidos são preliminares. Neste sentido, é fundamental a realização de novos testes, conforme previsto, para validar os aspectos de escalabilidade, confiabilidade e segurança, principalmente em função da sensibilidade dos dados. De forma complementar, aspectos de inteligência também deverão ser validados, à luz dos relatórios e notificações gerados, para que se verifique a eficácia dos resultados na prática cotidiana das investigações e exames periciais.

Do ponto de vista das limitações que forem observadas nos testes, alguns trabalhos podem adicionar importantes funcionalidades à plataforma, como é o caso da identificação automática de padrões em imagens e vídeos, que são evidências que podem ser registradas na plataforma. Além disso, a comunicação da plataforma com outras plataformas também pode ser explorada, especialmente com a implementação de funcionalidades de importação e exportação de dados, principalmente nos formatos CSV (*Comma Separeted Values*), XML (*Extensible Markup Language*) e JSON (*JavaScript Object Notation*). Por fim, o sistema de notificação da plataforma pode ser aperfeiçoado, entregando alertas aos usuários por *e-mail* ou até notificações *push* em dispositivos móveis.

Referências

ADEDAYO, O. M. Big data and digital forensics. In. [S.l.]: IEEE – International Conference on Cybercime and Computer Forensic, 2016. 3.

CAI D. LI, Y. W. Y. Intelligent crime prevention and control big data analysis system based on imaging and capsule network model. In: Neural Processing Letters. 53. ed. [S.l.: s.n.], 2020. p. 2485–2499. 3.

CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd. ed. Academic Press, 2017.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br). TIC Domicílios 2020. 2020. Disponível em: ⟨https://cetic.br/pesquisa/domicilios/2020/⟩.

CHERMAK, S. et al. Law enforcement's information sharing infrastructure: A national assessment. In: [S.l.: s.n.], 2013. v. 16, n. 2, p. 211–244.

HPE Security Research Cyber Risk Report 2022. Disponível em: <http://www8.hp.com/us/en/software-solutions/cyber-riskreport-security-vulnerability/>. Acesso em dezembro de 2022.

KANCA, S. A. M. Sharing cyber threat intelligence and collaboration. In: [S.l.]: IEEE – International Conference on Information Security and Cryptology, 2021.

MACHINA, A. A.; SONGJIANG, L. Crime analysis and intelligence system model design using big data. In: [S.l.: s.n.], 2020.

MARCO CIVIL DA INTERNET. Lei N° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Portal da Legislação, Brasília, abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 fev. 2023.

MCGARRELL, E. F.; FREILICH, J. D.; CHERMAK, S. Intelligence-led policing as a framework for responding to terrorism. In: [S.l.: s.n.], 2007. v. 23, n. 2, p. 142–158.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big Data: a revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013.

PRAMANIK RAYMOND Y. K. LAU, W. T. Y. Y. Y. C. L. M. I. Big data analytics for security and criminal investigations. In: [S.l.]: WIREs Data Mining and Knowledge Discovery, 2017.

SAFERNET. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em: <http://indicadores.safernet. org.br/>. Acesso em fevereiro de dezembro de 2022.

SEIDLER, R. A. P. Intelligence-led policing as a framework for responding to terrorism. In: International Journal of Police Science Management. [S.l.: s.n.], 2013. p. 323–337.

TREGLIA, J. V.; PARK, J. S. Towards trusted intelligence information sharing. In: Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics. New York, NY, USA: Association for Computing Machinery, 2009, (CSI-KDD '09). p. 45–52. ISBN 9781605586694. Disponível em: ⟨https://doi.org/10.1145/1599272.1599283⟩.

VELHO, Jesus Antonio (Org). Tratado de computação forense. Campinas: Millennium, 2016.