UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS REITOR JOÃO DAVID FERREIRA LIMA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
NÍVEL MESTRADO - MINTER – UFSC – PF

PAULO VITOR BRAGA DO NASCIMENTO

APRIMORAMENTO DA COLETA, GESTÃO E CADEIA DE CUSTÓDIA DE DADOS TELEMÁTICOS EM INVESTIGAÇÕES POLICIAIS:

Uma Abordagem Baseada em Blockchain.

FLORIANÓPOLIS
2024

PAULO VITOR BRAGA DO NASCIMENTO

APRIMORAMENTO DA COLETA, GESTÃO E CADEIA DE CUSTÓDIA DE DADOS TELEMÁTICOS EM INVESTIGAÇÕES POLICIAIS:

Uma Abordagem Baseada em Blockchain.

Dissertação submetida ao Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Ciência da Informação. Linha de Pesquisa: Dados, Inteligência e Tecnologia.
Orientador: Prof. Dr. Gustavo Medeiros de Araujo
Coorientador: Prof. Dr. Bruno Requião da Cunha

Florianópolis
2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.

Dados inseridos pelo próprio autor.

do Nascimento, Paulo Vitor Braga
APRIMORAMENTO DA COLETA, GESTÃO E CADEIA DE CUSTÓDIA DE DADOS TELEMÁTICOS EM INVESTIGAÇÕES POLICIAIS : Uma Abordagem Baseada em Blockchain / Paulo Vitor Braga do Nascimento ; orientador, Gustavo Medeiros de Araujo, coorientador, Bruno Requião da Cunha, 2024.
110 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós-Graduação em Ciência da Informação, Florianópolis, 2024.

Inclui referências.

1. Ciência da Informação. 2. Cadeia de Custódia. 3. Evidência Digital. 4. Blockchain. 5. Investigação Policial. I. de Araujo, Gustavo Medeiros . II. da Cunha, Bruno Requião . III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. IV. Título.

Paulo Vitor Braga do Nascimento

APRIMORAMENTO DA COLETA, GESTÃO E CADEIA DE CUSTÓDIA DE DADOS TELEMÁTICOS EM INVESTIGAÇÕES POLICIAIS:

Uma Abordagem Baseada em Blockchain.

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof.(a) Marcio Matias, Dr(a).
Universidade Federal de Santa Catarina

Prof.(a) Alex Sandro Roschildt Pinto, Dr(a).
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Mestre em Ciência da Informação.

Documento assinado digitalmente
Edgar Bisset Alvarez
Data: 30/10/2024 10:16:20-0300
CPF: ***.516.228-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Edgar Bisset Alvarez
Coordenador(a) do Programa

Documento assinado digitalmente
Gustavo Medeiros de Araujo
Data: 24/10/2024 12:10:35-0300
CPF: ***.754.991-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr.(a) Gustavo Medeiros de Araujo
Orientador(a)

Florianópolis, 16 de outubro de 2024.

Este trabalho é dedicado à minha esposa e aos meus filhos, assim como aos meus queridos pais, que desde cedo me ensinaram o valor da educação para compreender o mundo e, com muita paciência e amor, me mostraram que não há limites para a busca de um sonho.

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos a todas as pessoas que estiveram ao meu lado durante a elaboração desta dissertação.

Agradeço, em primeiro lugar, a Deus, por Sua constante orientação e inspiração. Sua presença divina e sabedoria iluminaram meu caminho, concedendo-me força e perseverança para enfrentar os desafios deste trabalho acadêmico. Obrigado por ser a minha força e guia em todos os momentos. A Ti, Senhor, toda honra e toda glória.

Aos meus pais, pelo apoio e incentivo em todos os momentos da minha vida. Sempre me incentivaram nos estudos e me ensinaram que, por meio da educação, podemos alcançar não só o aprimoramento intelectual, mas também o pessoal e humano. Agradeço por acreditarem em mim e por não medirem esforços, desde os primeiros anos de alfabetização, para que eu compreendesse a importância da educação na concretização dos meus sonhos. Sem vocês, nada disso seria possível. Mesmo com a distância que nos separa, vocês sempre estiveram presentes em minha vida e estarão eternamente em meu coração.

Agradeço à minha amada esposa, Marcela, cujo apoio e compreensão foram inestimáveis durante todo o processo. Seu amor incondicional, paciência e encorajamento foram um verdadeiro suporte emocional, motivando-me a dar o meu melhor em cada etapa.

Agradeço aos meus filhos, Nicolas e Lorenzo, que trouxeram alegria e inspiração para minha vida. Seus sorrisos, amor e energia positiva iluminaram meus dias e me impulsionaram a persistir, mesmo diante dos desafios. Eles suportaram, com compreensão, os momentos de ausência do pai nos períodos necessários aos estudos.

Por fim, agradeço aos meus amigos e colegas de trabalho, cujo apoio e encorajamento foram um verdadeiro bálsamo durante esta jornada acadêmica. Suas palavras de incentivo, discussões construtivas e motivação mútua foram essenciais para minha evolução e crescimento como profissional e pesquisador.

A todos os professores, orientador e coorientador, que contribuíram para minha jornada acadêmica, meu mais profundo agradecimento. Sem o apoio e conhecimento de cada um de vocês, este trabalho não teria sido possível.

E, finalmente, agradeço a todos que, mesmo não mencionados, foram colaboradores diretos ou indiretos desta pesquisa. Que nossa conexão continue a se fortalecer e que possamos compartilhar muitas conquistas e momentos de apoio mútuo ao longo de nossas vidas.

Com gratidão, Paulo Vitor.

THINKING

Se pensais em ser vencido, sereis;
Se pensais que não ousais, não ousareis;
Se quereis vencer, mas desanimais,
Provavelmente não vencereis.

Se pensais em perder, perdereis;
Pois é coisa sabida
Que o triunfo começa com um simples desejo
Num mero estado de espírito.

Se pensais que sois pária, sereis.
É preciso pensar em elevar-se, para tal conseguir;
É preciso estar certo de si mesmo
Para um prêmio poder alcançar.

A batalha da vida nem sempre é vencida
pelo mais forte ou o mais ágil,
Cedo ou tarde ***AQUELE QUE VENCE***
É O QUE PENSA QUE PODE VENCER*.*

Walter D. Wintle

"Todos honram aquele que conquista um prêmio",
É o que o mundo proclama há milhares de anos;
Mas ao que tenta, fracassa e morre,
Honro e glorifico com lágrimas.
Glorifiquemos e honremos com piedosas lágrimas
Os que fracassam em feito sublime;
Suas almas estão na vanguarda dos anos,
Eles nasceram com o Tempo, ou o precederam.

Grande é o herói que conquistou um nome;
Porém maior, muitas vezes maior,
É o ser pálido e triste que morre no opróbrio,
E deixa a Deus completar sua ideia sublime.
Bravo é o homem que a espada desembainha,
E virtuoso aquele que do vinho se abstém;
MAS O QUE FRACASSA E PROSSEGUE LUTANDO,
ESTE SIM, É QUE É O MEU IRMÃO GÊMEO.

Joaquin Miller, ***Poet of the Sierras***

RESUMO

A investigação policial, no contexto da revolução digital, passou a lidar com evidências criminais provenientes de diversas fontes tecnológicas, o que frequentemente exige medidas judiciais para obtenção desses dados junto a empresas de tecnologia e seus armazenamentos em nuvem. A gestão dessas evidências digitais enfrenta desafios críticos e atuais, especialmente na garantia da cadeia de custódia. A inexistência de padronização nos processos de aquisição, arquivamento digital e armazenamento pode comprometer a integridade das provas, conforme reconhecido em recentes decisões judiciais, onde a quebra da cadeia de custódia levou à invalidação de provas essenciais para a persecução penal. Este trabalho, respaldado por pesquisa diagnóstica institucional e bibliográfica, descreve as principais dificuldades enfrentadas na gestão das evidências digitais oriundas da quebra de sigilo telemático. A partir da análise desses desafios, propõe-se uma plataforma Web baseada na tecnologia Blockchain, que visa aprimorar o ciclo de vida e o uso dos dados telemáticos obtidos judicialmente, garantindo a imutabilidade, a integridade e a rastreabilidade das evidências ao longo de todo o processo judicial. A solução proposta busca mitigar os problemas de fragilidade na gestão de dados, fornecendo uma estrutura robusta e alinhada às exigências legais e operacionais da investigação criminal no Brasil.

Palavras-chave: Cadeia de Custódia, Evidência Digital, *Blockchain*, Solicitações judiciais, Investigação Policial.

ABSTRACT

In the context of the digital revolution, police investigations have increasingly dealt with criminal evidence from various technological sources, often requiring judicial measures to obtain this data from technology companies and their cloud storage systems. Managing this digital evidence presents critical and current challenges, particularly in ensuring the chain of custody. The lack of standardization in acquisition, digital archiving, and storage processes can compromise the integrity of the evidence, as recognized in recent judicial decisions, where breaches in the chain of custody have led to the invalidation of essential evidence for criminal prosecution. This study, supported by institutional diagnostic research and a bibliographic review, describes the main difficulties faced in managing digital evidence resulting from telematic data breaches. Based on the analysis of these challenges, a Web platform based on Blockchain technology is proposed, aiming to enhance the lifecycle and use of telematic data obtained through judicial processes, ensuring the immutability, integrity, and traceability of evidence throughout the judicial process. The proposed solution seeks to mitigate the fragility in data management by providing a robust framework aligned with the legal and operational requirements of criminal investigations in Brazil.

Keywords: Chain of Custody, Digital Evidence, *Blockchain*, Law Enforcement Requests, Police Investigation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANCIB – Associação Nacional de Pesquisa e Pós-graduação em Ciência da Informação

API – *Application Programming Interface* ou Interface de Programação de Aplicação

BNDES – Banco Nacional de Desenvolvimento Econômico e Social

BPMN – *Business Process Model and Notation* ou Notação da Modelagem de Processos do Negócio

CD-Rs – *Compact disc-recordable*

CD-RWs – *Compact Disc ReWritable*

CDs – *Compact Discs*

CoC – *Chain of Custody* ou Cadeia de Custódia

CPP – Código de Processo Penal

DLT – *Distributed Ledger Technology* ou Tecnologia de Ledger Distribuído

DVDs – *Digital Versatile Discs*

EVM – *Ethereum Virtual Machine* ou Máquina virtual *Ethereum*

HDs – *Hard Disk*

IA – Inteligência Artificial

IN – Instrução Normativa

PoA - *Proof-Of-Authority* ou Prova de Autoridade

RBB – Rede *Blockchain* Brasil

REST – *Representational State Transfer* ou Transferência de Estado Representacional

RPA - *Robotic Process Automation* ou Automação Robótica de Processos

SGD – Secretaria de Governo Digital

SSDs – *Solid State Drive*

SSPs – *Storage Service Providers*

TA – *Trusted Agent* ou Autoridade Confiável

TCU – Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO

A popularização da internet e de seu uso por dispositivos móveis já passou a fato cotidiano. O uso intensivo de redes sociais, comunicações instantâneas, aplicativos de diversas funcionalidades, e a troca constante de informações em áudio e vídeo quase em tempo real, juntamente com transmissões de canais pessoais, já vinha crescendo significativamente. A execução de várias tarefas de forma remota também se tornou comum. Esse cenário foi ainda mais intensificado pela pandemia global, que forçou a adaptação rápida de atividades presenciais para o ambiente virtual, criando um universo informacional ainda mais vasto e complexo. A pandemia acelerou a digitalização em várias esferas, resultando em um aumento expressivo na geração e no armazenamento de dados, o que trouxe novos desafios para a gestão e a segurança dessas informações. As crescentes informações oriundas do armazenamento de dados em nuvens, bancos de dados com informações criminais, relatórios de informações financeiro-patrimoniais, entre outros, são fontes de informações importantes na investigação e na solução de crimes, além de ajudarem a compor evidências nos processos judiciais e orientar estratégias no combate à criminalidade.

Nesse cenário, os órgãos de segurança pública identificaram novas possibilidades de afastamento de sigilo, mediante ordem judicial, junto às empresas de tecnologia. A legislação brasileira permite avançar neste sentido, a partir do momento em que se pode afastar o sigilo de registros de acesso de aplicações de Internet, além da requisição de dados cadastrais e conteúdo armazenado. Naturalmente, passando a lidar com esse repositório investigativo como fonte de evidências criminais.

Essa enxurrada tecnológica produz maciçamente milhares de dados diariamente, implicando a necessidade de gerir e processar tais dados. A necessidade de aprimorar e até aprender a conviver com esse diverso e complexo volume de dados que exige recursos tecnológicos e metodologia adequada é fundamental para recuperar e transformar em informação útil ao contexto policial (BARTH *et al*., 2007). Porém, o volume, complexidade e dispersão desses dados ainda dificultam o trabalho policial de investigação, exigindo sobretudo infraestrutura para trato com esses dados, além da garantia da integridade e autenticidade da evidência digital em todo o ciclo da persecução criminal.

Ainda precisa ser considerado, conforme esclarecem Martins e Vianna (2019), o paradigma cognitivo da informação, que considera os modelos mentais dos usuários, utilizando

abordagens cognitivas, centradas no processo interpretativo do sujeito cognoscente sobre a informação que é produzida. A inexistência de padronização e metodologia técnica direciona cada investigador a gerir individualmente, conforme sua cognição ou política local, a aquisição e o arquivamento digital, a cadeia de custódia da prova[1], dificultando, ainda, a integração das evidências digitais oriundas de múltiplas instâncias. Promove dificuldade para uma recuperação inteligente da informação ou uso de ferramentas de Inteligência Artificial (IA) e Mineração de Dados. Além disso, gera o risco do arquivamento digital inadequado e na possível violação da cadeia de custódia da evidência criminal.

Neste ponto, a evidência digital poderia ser direcionada ao especialista forense, para processá-la e devolvê-la pronta ao investigador para análise; entretanto, a demanda para este tipo de trabalho é alta e exige sua célere análise. Isso resulta em excessiva demanda caso direcionada somente ao perito forense, sem mencionar que a aquisição dos dados ainda ficaria a cargo do investigador. Abre-se, desta forma, uma nova frente de trabalho para o investigador, a gestão direta daquela evidência digital e de sua cadeia de custódia.

Os autores Milagre e Segundo (2015, p. 36-37) descreveram, de forma bem apropriada, os desafios atuais para a perícia em informática envolvendo a análise de grandes volumes de dados, em que há enorme similaridade com o cenário estudado neste trabalho, como descrito:

> **a) A grande quantidade de dados em formatos diferenciados, textos não estruturados e arquivos multimídia: Coletar informações *Web* ou em rede implica estar preparado para lidar com inúmeros formatos e principalmente, para lidar ou interpretar imagens e conteúdos visuais e dados não estruturados;**
>
> **b) A ausência de profissionais atuando em Computação Forense que compreendam conceitos e técnicas da Ciência da Informação (metadados, ontologias, arquitetura da informação, métodos de indexação, estudo quantitativos e sobre recuperação da informação, entre outros) e que possam desenhar as melhores técnicas para tratamento da informação relevante a uma investigação;**
>
> **c) A ausência de fontes únicas de dados, sendo que uma perícia envolvendo Big Data pode recair sobre toda a Internet, tráfego de rede interno, redes sociais, mecanismos de busca ou mesmo sobre arquivos e e-mails armazenados em um dispositivo de armazenamento;**
>
> **[...]**
>
> **d) A ausência de cooperação por parte dos provedores de serviços que hospedam ou armazenam os dados gerados por suspeitos, como a ausência de um padrão para interconexão com autoridades e**

[1] Cadeia de Custódia: Conjunto de procedimentos destinados a preservar e documentar a integridade de uma evidência, registrando todas as etapas de manuseio desde a coleta até a sua apresentação em juízo, conforme definido no artigo 158-A do Código de Processo Penal (Lei nº 13.964/2019).

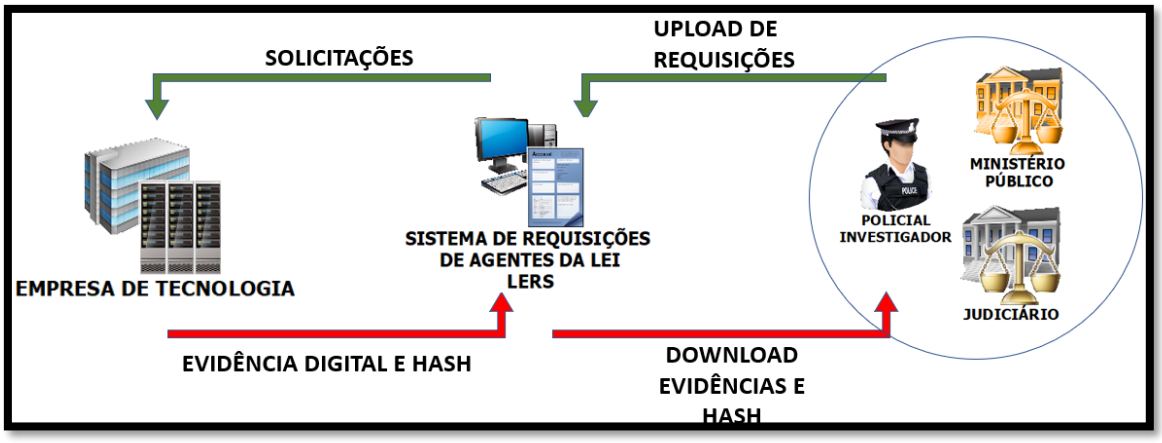
> **investigadores, para manipulação a tais dados.**
>
> O rol citado, meramente exemplificativo, elucida os desafios que a Perícia em Informática ou Computação Forense enfrenta ao se deparar com *terabytes* de dados e informações, sendo muitas vezes informações dispostas na Internet e em ferramentas de redes sociais de forma desestruturada.
>
> [...]
>
> **O emprego e revisão dos processos de investigação, aplicando-se o aporte de áreas de estudo da Ciência da informação, como protocolos, metadados, ontologias, técnicas de indexação, estudos quantitativos e as tecnologias da *Web* semântica podem ser fortes aliados no aprimoramento da atividade da computação forense.** (Grifo nosso)

Na pesquisa realizada por Milagre e Segundo (2015, p. 36-37), foram apontados relevantes pontos convergentes, como a ausência de um padrão para interconexão com autoridades e investigadores, para manipulação dos dados das evidências digitais, o problema do armazenamento, os atores envolvidos e garantia da custódia, bem como outros desdobramentos.

Esse ambiente é semelhante ao trabalho com os arquivos gerados pelas medidas cautelares de quebra de sigilo telemático, atividade comum do investigador na qual a investigação criminal espera prosperar obtendo evidências para persecução criminal com o uso destas fontes tecnológicas.

Com o aumento da demanda por parte da segurança pública, a maioria das grandes empresas de tecnologia precisou se especializar no atendimento dessas requisições, adotando sistemas como o LERS (Law Enforcement Request System), uma plataforma web que permite aos agentes da lei enviarem, de forma segura, solicitações legais de dados, acompanhar o status dessas solicitações e fazer o download dos dados telemáticos. No entanto, o LERS, embora facilite a requisição e o recebimento de dados, não resolve as questões relacionadas à gestão interna dessas evidências. A inexistência de uma ferramenta tecnológica ou de um sistema automatizado que permita a aquisição padronizada, o arquivamento digital adequado, o armazenamento e a gestão de acesso às evidências recebidas do LERS ainda prejudica a investigação criminal. Isso ocorre porque, após o recebimento dos dados, o processo continua a ser manual e despadronizado, ficando a cargo de cada investigador, o que fragiliza a cadeia de custódia e pode comprometer o processo legal.

Figura 1 - Plataforma de requisições das empresas de tecnologia



Fonte: Elaborado pelo autor (2022).

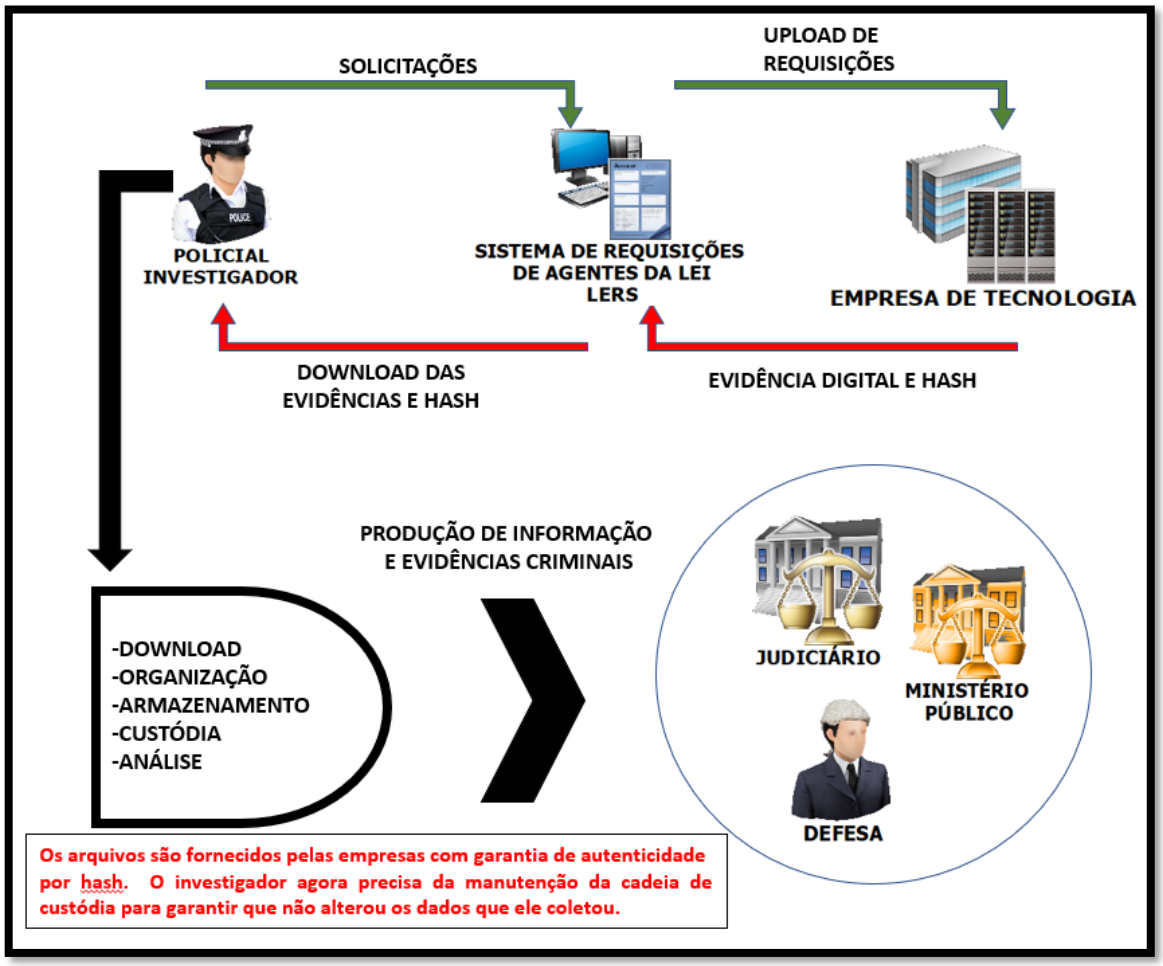
Desta forma, autoridades podem realizar requisições e receber os dados, extraídos de forma forense, diretamente. Destacamos, que neste processo normalmente não aparece a figura do perito forense. Fica claro que, na cadeia de custódia de evidências digitais, existe uma necessidade premente de manter a integridade das informações de uma maneira confiável e transparente. Geralmente, um valor *hash* de evidência digital é calculado e documentado com os dados adquiridos para provar que não foi alterado. No entanto, o valor de *hash* sozinho não prova que a evidência digital é a mesma de quando foi obtida, apenas que o conteúdo não foi modificado desde o momento em que o *hash* foi calculado (BURRI, X. *et al.,*2019).

Na imagem apresentada (figura 1), as autoridades da lei por meio de seus representantes realizarão o procedimento de aquisição das evidências por meio de download diretamente da plataforma, momento em que o manuseio e a organização dos arquivos podem comprometer a cadeia de custódia.

Com o desdobramento da nova frente de trabalho, as equipes de investigação começaram a lidar, em seu cotidiano, com todo o processo envolvido na produção deste tipo de prova, realizando todo o procedimento de requisição e recepção (aquisição) dos dados junto às plataformas das empresas de tecnologia, seu armazenamento e manutenção da cadeia de custódia além da análise e produção de conhecimento.

A inexistência de ferramenta tecnológica ou automatização para aquisição, arquivamento digital, armazenamento e gestão do acesso a essas evidências pode prejudicar a investigação criminal, devido ao procedimento sem padronização e manual (realizado pelo investigador), que cria um ambiente fragilizado ao processo legal e um problema a ser resolvido.

Figura 2 - Rotina na obtenção de evidências digitai



Fonte: Elaborado pelo autor (2022).

Apresenta-se acima (Figura 2) a rotina do investigador requisitando os dados de interesse de uma investigação criminal, por meio de uma autorização judicial, que é carregada na plataforma web (LERS) da empresa de tecnologia. Depois do processamento pela empresa, ele recebe, por meio de *download* na plataforma, os dados requisitados.

A partir desse momento, a cadeia de custódia se mostra essencial para o processo de registro e preservação de detalhes de evidências digitais desde a coleta/armazenamento até a entrega ao Judiciário e demais personagens envolvidos na persecução criminal. Trazendo ao foco deste trabalho, sugere-se, no cenário da investigação policial, uma arquitetura de gestão dos dados telemáticos que aprimore esse ambiente e garanta que as evidências fornecidas permaneçam originais e autênticas e armazenadas de forma segura, apoiada na tecnologia *Blockchain* como mantenedora da cadeia de custódia. Essa tecnologia é conhecida por sua imutabilidade, integridade, disponibilidade, autenticidade, irretratabilidade de seus dados em rede, principais razões que a levam a interagir com a gestão de evidências digitais.

É de extrema importância garantir integridade, autenticidade e auditoria de evidências digitais à medida que se move em diferentes níveis de hierarquia, ou seja, dos investigadores que obtêm a prova, até ao Judiciário, Ministério Público, Defesa, todos os envolvidos na persecução criminal e na cadeia de custódia. E o envolvimento por múltiplas partes neste processo, já se associa um risco de adulteração, implicando no principal problema, a documentação e registro das interações com a evidência. Por meio da tecnologia *Blockchain,* existe a possibilidade de se criar um livro-razão completo de todas as interações com a evidência de forma segura e inalterável.

A pesquisa exigiu conhecer o modelo do ciclo de vida das evidências digitais (dados telemáticos) usados na investigação atualmente. Foi necessário compreender a influência da inadequação da gestão nas etapas de aquisição, arquivamento digital e armazenamento adequado daqueles dados. E ainda, foi proposto um modelo de arquitetura para gerir esses arquivos digitais, especialmente os oriundos das medidas cautelares de quebra de sigilo de dados telemáticos. A elaboração de um sistema com a arquitetura proposta resolveria a questão do processo manual e individual do investigador (própria expertise) na aquisição, no arquivamento digital, no armazenamento dos dados e na gestão da cadeia de custódia da evidência digital.

1.1 DESCRIÇÃO DO PROBLEMA

A cadeia de custódia é uma técnica básica nas Ciências Forenses em qualquer área de atuação, um conjunto de procedimentos cuja finalidade é manter e registrar a história cronológica do vestígio e suas interações (posse e manuseio) com os que trabalham com ela. Desta forma, mantém-se a rastreabilidade a partir de sua coleta, processamento, até o descarte. E finalmente, um resultado é apresentado na forma de laudo com um parecer sobre a evidência examinada. As evidências devem ser manuseadas de forma cautelosa, e todo o manuseio na evidência deverá ser registrado na cadeia de custódia.

Em 10 de fevereiro de 2023, o *site* Migalhas[2] noticiou a decisão do Superior Tribunal de Justiça, quando a 5ª turma do STJ firmou importante precedente sobre a cadeia de custódia de prova digital.

[2] https://www.migalhas.com.br/quentes/381258/stj-invalida-prova-digital-por-quebra-de-cadeia-de-custodia

> A 5ª turma do STJ firmou importante precedente sobre cadeia de custódia de prova digital. O RHC (Recurso em *Habeas Corpus*) julgado envolvia paciente suspeito de fazer parte de quadrilha de hackers que desviava dinheiro da conta bancária de terceiros. Com voto condutor do ministro Ribeiro Dantas, o colegiado entendeu **pela inadmissibilidade de prova digital contaminada pela quebra da cadeia de custódia durante as fases de coleta, manutenção e manuseio dos dados.** (MIGALHAS, 2023). (Grifo nosso)

Figura 3 - Site Migalhas noticiou a invalidação das evidências digitais

Fonte: https://www.migalhas.com.br/quentes/381258/stj-invalida-prova-digital-por-quebra-de-cadeia-de-custodia

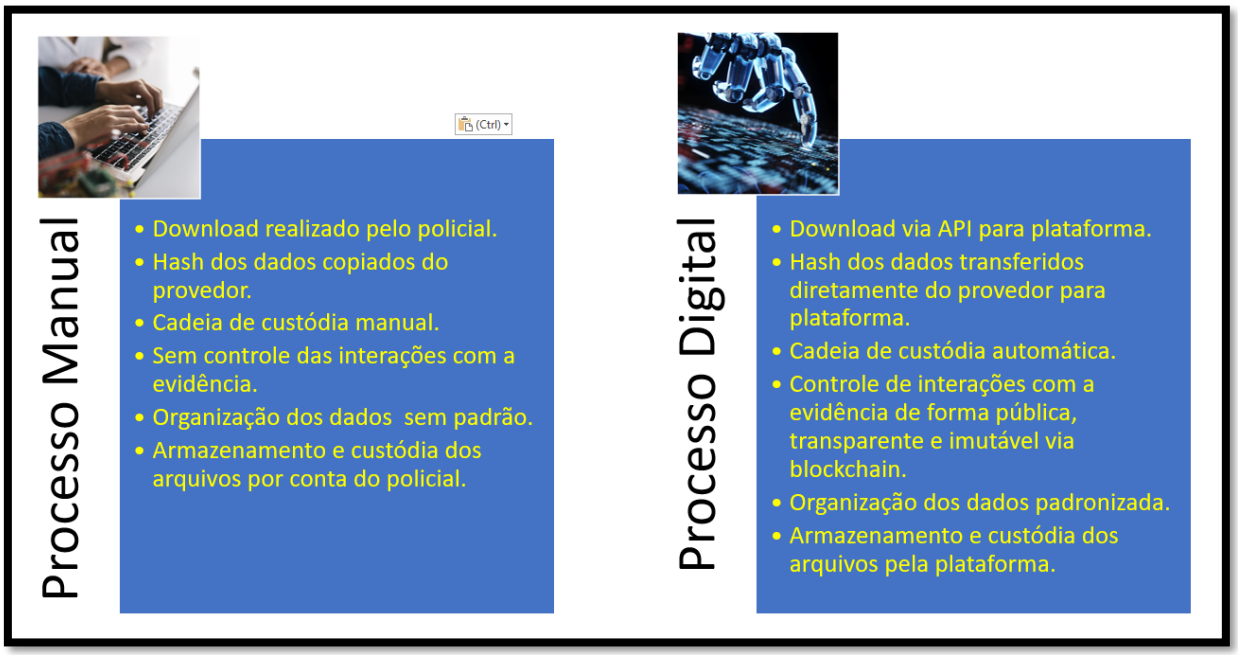
Recentemente, o arcabouço legal brasileiro confirmou que o trato com evidências digitais nas suas fases de coleta, manutenção e manuseio dos dados é de extrema relevância. Principalmente para investigadores não peritos, cujo trato com os dados de forma inadequada pode levar à anulação de todo o processo legal, por contaminar a cadeia de custódia da prova criminal. Com a revolução digital, cada vez mais evidências criminais digitais surgem no

cenário investigativo cotidiano e, consequentemente, mais investigadores e não peritos forenses passaram a lidar com essa realidade.

1.2 JUSTIFICATIVA DO TEMA

No contexto abordado, não há uma metodologia ou ferramenta tecnológica (plataforma) padronizada para adquirir, arquivar digitalmente e gerir o acesso às evidências digitais, especialmente no caso de medidas cautelares de quebra de sigilo telemático. O processo é realizado de forma manual e sem padronização, cabendo a cada investigador gerenciar as etapas de aquisição, arquivamento digital, armazenamento e a cadeia de custódia da prova. Esse cenário compromete a eficiência da persecução criminal e dificulta a formação de um corpus nacional de evidências digitais, essencial para o uso em ferramentas de IA.

Figura 4 - Antes e depois da pesquisa



Fonte: Elaborado pelo autor (2022)

A representação gráfica acima (Figura 3) descreve as diferenças do cenário atual sem uma ferramenta tecnológica e o cenário pretendido com o uso de uma ferramenta tecnológica voltada à gestão dos dados telemáticos apoiada em tecnologia *Blockchain*.

1.3 DELIMITAÇÃO DO ESCOPO

Esta pesquisa pretende descrever o fluxo do processo de gestão dos dados telemáticos obtidos judicialmente na investigação criminal brasileira e seus principais problemas baseados em avaliação diagnóstica na Polícia Federal do Brasil. A partir disso propor uma solução automatizada para o processo apoiada na tecnologia blockchain, com sugestão de um *framework* da arquitetura, acompanhada de um esquema de histórias de usuários com requisitos funcionais.

Está ausente do escopo deste trabalho o desenvolvimento definitivo e completo da plataforma pretendida, principalmente devido ao alcance e envolvimentos interinstitucionais. Essa ação, inexistente no contexto atual do trabalho, exigiria uma integração entre as partes interessadas e usuárias do sistema para um alinhamento comum mínimo.

Também estão fora do escopo deste trabalho os debates técnicos aprofundados sobre os mecanismos e aspectos de organização da informação ou do conhecimento, o que abre uma possibilidade para outros pesquisadores e trabalhos futuros. Ao se tratar de organização neste trabalho, definiu-se como pressuposto a organização mínima para o arquivamento digital, de forma a evitar a dispersão dos dados e uma recuperação da informação facilitada dentro da plataforma proposta.

1.4 OBJETIVOS

Os objetivos foram direcionados na busca de respostas para as questões a seguir.

A aquisição e o arquivamento digital das evidências digitais, dos dados obtidos pela quebra de sigilo telemático[3] envolvidos na investigação policial podem influenciar na persecução criminal?

Como eliminar o processo manual e individual do investigador (sua própria expertise) na gestão dos dados e da cadeia de custódia daquelas evidências digitais?

[3] Sigilo telemático é regido pelo Marco Civil da Internet, Lei 12.965/14, que regulam dados telefônicos e da internet, respectivamente. Neles, é estabelecido que, se a justiça exigir a quebra de sigilo de uma pessoa, que deve ser identificada na ação, as empresas são obrigadas a fornecer os dados para o magistrado.

1.4.1 Objetivo Geral

Propor uma solução automatizada para a gestão da cadeia de custódia dos dados telemáticos obtidos judicialmente na investigação criminal brasileira, descrevendo o fluxo do processo e os principais problemas identificados com base na avaliação diagnóstica da Polícia Federal e na literatura existente, utilizando a tecnologia blockchain.

Adicionalmente, ainda que não seja o foco principal, a pesquisa visa produzir um *framework*[4] para a arquitetura da solução proposta. Esse framework incluirá um esquema de histórias de usuários com funcionalidades, alinhado à metodologia de desenvolvimento ágil[5]. O objetivo é fornecer uma base para a posterior criação de uma plataforma corporativa escalável para a gestão de dados telemáticos[6], abrangendo a aquisição, o arquivamento digital e o pré-processamento. Esses elementos fornecerão a estrutura necessária para o desenvolvimento final da solução em qualquer ambiente.

1.4.2 Objetivos Específicos

São objetivos específicos do presente trabalho:

a. Esquematizar, por meio de fluxo de processo, o modelo do ciclo de vida das evidências digitais, os dados de quebra de sigilo telemático usados na investigação atualmente;

b. Identificar os principais pontos de fragilidade nos trabalhos com dados de quebra de sigilo telemático;

---

[4] Na linguagem de programação, um framework é uma estrutura de suporte composta por um conjunto de classes abstratas e interfaces, que fornecem soluções genéricas para problemas comuns de desenvolvimento. Ele serve como base para a construção de sistemas, oferecendo funcionalidades reutilizáveis, o que acelera o processo de desenvolvimento ao padronizar partes do código. **Fonte**: JACQUES, Jean. O que é um framework? Departamento de Sistemas e Computação, Universidade Federal de Campina Grande. Disponível em: http://www.dsc.ufcg.edu.br/~jacques/cursos/map/html/frame/oque.htm.

[5] Desenvolvimento Ágil é uma abordagem que utiliza processos e práticas que promovem a entrega contínua de software de qualidade, ajustando-se rapidamente a mudanças de requisitos ao longo do ciclo de desenvolvimento. **Fonte**: BECK, Kent et al. Manifesto for Agile Software Development. 2001. Disponível em: https://agilemanifesto.org/

[6] Telemática refere-se à integração entre telecomunicações e informática para fornecer serviços à distância, utilizando redes de comunicação para conectar dispositivos e compartilhar dados em tempo real. **Fonte**: STALLINGS, William. Data and Computer Communications. Pearson Education, 2020.

c. Demonstrar as dificuldades internas de gestão dos dados de quebra de sigilo telemático usados na investigação apoiado em pesquisa diagnóstica na Polícia Federal;

d. Examinar trabalhos relacionados apoiados na tecnologia *Blockchain* como mantenedora da cadeia de custódia das evidências digitais;

e. Esboçar um *framework* de arquitetura, apoiado na tecnologia Blockchain, que permita a automatização e garanta a integridade da cadeia de custódia para a aquisição, o arquivamento digital e a gestão de todos os registros de manuseio dos dados pelos diversos atores envolvidos no processo.

1.5 ORIGINALIDADE E CONTRIBUIÇÕES DA PESQUISA

Apesar da proteção da cadeia de custódia por meio da tecnologia *Blockchain* encontrar diversos casos na literatura, a originalidade do presente estudo está no processo de obtenção dos dados oriundos de uma quebra de sigilo telemático em uma investigação policial e na avaliação diagnóstica interna desse processo em uma instituição policial.

A gestão da cadeia de custódia por meio da tecnologia *Blockchain* é apontada nas pesquisas como uma excelente solução para o cenário em tela, sendo inexistente no cenário da investigação criminal brasileira e uma grande evolução no processo criminal brasileiro e inovação no campo da Ciência Policial.

Há estudos que demonstram que o uso de *Blockchain* pode garantir a integridade da cadeia de custódia para que possam ser aceitas judicialmente, além de preservar a autenticidade e manter a rastreabilidade dos envolvidos com as evidências digitais (ANNE *et al.*, 2021; LI *et al.*, 2021; BONOMI, S. *et al.*, 2020; TIAN *et al.*, 2019; CHOPADE *et al.*, 2019; GOPALAN *et al.*, 2019).

Como exemplo, os diversos estudos selecionados apontam que, em processos de custódia de evidências digitais, a tecnologia *Blockchain* é uma estrutura escalável, garante a integridade e validade das evidências e equilibra bem a privacidade e a rastreabilidade.

Nesse contexto, em decorrência de pesquisar a interação do cenário investigativo que envolve a quebra de sigilo telemático, encontramos uma lacuna a ser preenchida. Nesse

momento o investigador, numa gestão individual e manual da evidência digital, reduz sua produtividade e fragiliza a cadeia de custódia, por inexistência de uma metodologia técnica e forense adequada para a aquisição, arquivamento digital, guarda e armazenamento dos dados, além da gestão das interações com essas evidências.

1.6 ORGANIZAÇÃO DA PESQUISA

Este trabalho foi organizado da seguinte forma. Após a introdução, na seção 2, apresentamos os fundamentos teóricos. Na seção 3, são descritos a metodologia do trabalho dividida em três pontos: mapeamento da literatura, avaliação diagnóstica e modelagem do processo. Na seção 4 temos os trabalhos relacionados, resultado do mapeamento da literatura. A descrição do ciclo de vida dos dados telemáticos e o fluxo de seu processo são descritos na seção 5. A seção 6 mostra os resultados da avaliação diagnóstica. Na seção 7, apresentamos algumas conclusões. Na seção 8, apresentamos um modelo e sua arquitetura para solucionar o problema da pesquisa. Algumas considerações são apresentadas na seção 9.

1.7 ADERÊNCIA DO TEMA À CIÊNCIA DA INFORMAÇÃO

A Ciência da Informação nasceu num cenário onde conseguia administrar, a geração e a organização da informação e, numa outra vertente, a transferência, preservação e recuperação da informação mediada pela tecnologia:

> A Ciência da Informação é a disciplina que investiga as propriedades e o comportamento informacional, as forças que governam os fluxos de informação, e os significados do processamento da informação, visando à acessibilidade e a usabilidade ótima. [...] está preocupada com o corpo de conhecimentos relacionados à origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação. [...] uso de códigos para a transmissão eficiente da mensagem, bem como o estudo do processamento e de técnicas aplicadas aos computadores e seus sistemas de programação (BORKO, 1968, p. 1-2).

A necessidade de gerir e organizar a informação de forma metódica e científica data de muito tempo, e há muito já se planejava executar tais tarefas com auxílio de tecnologia computacional. Ainda conforme o entendimento de Saracevic (1996 apud MOOERS, 1951), o futuro uso do *Big Data* poderia ser estruturado pela Ciência da Informação, sendo até hoje peça-chave na recuperação de informação por meios tecnológicos.

> Considerando o problema da informação definido, isto é, a explosão informacional, a recuperação da informação tornou-se uma solução bem-preparada encontrada pela CI e em processo de desenvolvimento até hoje. Como toda solução suscita seus próprios e específicos problemas, assim também a recuperação da informação" e esses problemas estão contidos na concepção proposta por Mooers: a) como descreve intelectualmente a informação / b) como especificar intelectualmente a busca? / c) que sistemas, técnicas ou máquinas devem ser empregados? (SARACEVIC, 1996, p. 44)

A Ciência da Informação exerce papel fundamental, pois seus estudiosos começaram com uma vantagem competitiva em relação ao *Big Data*: sabiam como armazenar, gerenciar e processar dados; e entendiam a complexidade das estruturas de dados muito cedo na história da Ciência da Informação. Conheciam, ainda, os desafios associados à infraestrutura necessária para lidar com o volume de dados que está sendo gerado hoje (AGARWAL; DHAR, 2014).

A Ciência da Informação pode ser considerada como uma ciência multi e interdisciplinar, característica-chave para lidar com um universo informacional tão diverso em sua estrutura e conteúdo como é o caso de *datasets* complexos. Como assevera Saracevic (1995), a Ciência da Informação possui três características fundamentais: sua interdisciplinaridade, sua inexorável conexão com a tecnologia da informação e ainda uma ativa participação na evolução da sociedade da informação.

Desta forma, a obtenção, representação, armazenamento, disseminação e consumo dessa gigantesca massa dispersa de dados usada na investigação policial podem ser auxiliados pela Ciência da Informação na produção, organização e recuperação da informação, principalmente por seu eixo tecnológico de informação e tecnologia, delineado pela ANCIB[7] em seu percurso temático do Grupo de Trabalho – GT 08. As tecnologias de tratamento de dados como a Ciência de Dados, Inteligência Artificial e tecnologias afins são ferramentas capazes de acelerar o processo de investigação, poupando horas do trabalho dos agentes, aumentando a probabilidade de prisões em flagrante e a recuperação de bens, entre outros benefícios.

A extração de evidências e correlações relevantes para o processo investigativo requer o apoio desde a etapa de armazenamento e integração entre diferentes bases de dados, até a etapa de análise estatística e descoberta de padrões. E também para as mais diversas finalidades,

[7]Associação Nacional de Pesquisa e Pós-graduação em Ciência da Informação – ANCIB - Grupo de Trabalho GT 08 - Estudos e pesquisas teórico-práticos sobre e para o desenvolvimento de tecnologias de informação e comunicação que envolvam os processos de geração, representação, armazenamento, recuperação, disseminação, uso, gestão, segurança e preservação da informação em ambientes digitais (http://gtancib.fci.unb.br/index.php/gt-08).

como seu uso em reconhecimento facial, detecção de padrões criminais georreferenciados, mineração de texto e reconhecimento de escrita e áudio, além de diversas outras aplicações.

Nesse sentido, a investigação criminal de melhor qualidade visará à recuperação da informação de forma pragmática, a fim de subsidiar o processo de persecução penal, alterando a estrutura de conhecimento sobre o indivíduo que é investigado. Assim, a inserção dos pressupostos da Ciência da Informação na investigação criminal poderá servir ao desenvolvimento de sua efetividade teleológica, no intuito de produzir e recuperar informações essenciais na persecução penal de maneira eficiente, gerada dentro de seus processos e procedimentos (MARTINS; VIANNA, 2019).

Entretanto, alguns pontos ainda precisam ser observados, como a maturidade tecnológica e de recursos humanos qualificados para tratar deste assunto.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, serão discutidos os principais conceitos e definições relativos aos assuntos discutidos neste trabalho e oriundos de referências teóricas sobre o tema proposto, através de livros, *sites* especializados, artigos científicos e dissertações, aprofundando o embasamento teórico para a pesquisa. A pesquisa documental vale-se de materiais que ainda não receberam nenhuma análise aprofundada

2.1 A INVESTIGAÇÃO CRIMINAL E OS DADOS DE FONTES TECNOLÓGICAS

Os dados são considerados o novo petróleo da era digital, embora não exista uma universalização do conceito de *Big Data*, sobretudo no meio acadêmico, por se tratar de um termo relativamente novo (DE SOUZA, 2018). O crescimento e a integração de grandes volumes de dados digitais – vulgarmente chamado *Big Data* – têm sido utilizados para a tomada de decisão em diferentes áreas.

2.1.1 Os dados de fontes tecnológicas – *Big Data*

Não é novidade no campo da Administração e da Ciência da Informação a proposta de utilização de grande quantidade de informações; no entanto, esse cenário se tornou mais evidente e forte a partir dos anos 1950, com a maior utilização de sistemas de informação pelas empresas (CHEN; CHIANG; STOREY, 2012).

Um dos entendimentos descritos por Manyika *et al*. (2011) seria que *Big Data* se refere ao conjunto de dados (*dataset*) cujo tamanho está além da habilidade de ferramentas típicas de banco de dados em capturar, gerenciar e analisar. A definição é intencionalmente subjetiva e incorpora uma definição que se move de como um grande conjunto de dados necessita ser para ser considerado um *Big Data*. Tal entendimento se coaduna com o volume de informações envolvidas numa investigação policial.

Atualmente, o termo *Big Data* encontra-se disperso em ramos tão diversificados como o da informática, medicina, economia, gestão, biologia, segurança, entre incontáveis outros. Embora seja utilizado nesta quantidade vastíssima de áreas, este não afeta todos da mesma forma (MANYIKA *et al*., 2011).

Agarwal e Dhar (2014) descrevem muito bem o cenário atual quando mencionam que a capacidade de compreender a estrutura e o conteúdo do discurso humano expandiu consideravelmente a dimensionalidade dos conjuntos de dados disponíveis. Como resultado, o conjunto de oportunidades de investigação explodiu exponencialmente com conjuntos de dados grandes e complexos prontamente disponíveis relacionados a qualquer tipo de fenômeno que os pesquisadores queiram estudar. O uso de *Big Data* na segurança pública é inevitável e tornou-se um campo fértil para ser explorado cada vez mais pelos pesquisadores, e certamente seria produtivo também se mais bem direcionado à investigação policial.

Sob um outro aspecto, o uso de dados de fontes tecnológicas está em pleno desenvolvimento e exige infraestrutura e recursos humanos qualificados para seu manuseio no Brasil e até na Europa. Neiva (2020) avalia o cenário europeu, em seu artigo intitulado “Big Data na investigação criminal”, no qual menciona as expectativas dos meios de investigação atuais, que carecem de desenvolvimento informático para que o *Big Data* se materialize, encontrando eco nas restantes categorias profissionais entrevistadas em seu trabalho. Estas também consideram que se trata de uma ferramenta mais avançada do que o contexto em que opera e, por isso, exige que o meio onde se insere se desenvolva para que se possa efetivar. Por

este motivo, não tem ampla aplicação atualmente e é necessário o desenvolvimento dos profissionais, das áreas, dos métodos e do meio. Ou seja, há uma concessão generalizada de que se trata de uma técnica em desenvolvimento na esfera da investigação criminal: um conhecimento em construção. O policial investigador da atualidade precisa de capacitação técnica para lidar com esse novo contexto ou de ferramentas que auxiliem nesse cenário tecnológico.

2.1.2 Os dados de fontes tecnológicas – a investigação criminal

As investigações policiais contemporâneas envolvem a análise de uma enorme quantidade de dados, em múltiplos formatos, originados de três fontes básicas: (i) humanas; (ii) de conteúdo; e (iii) tecnológicas. As fontes humanas podem ser determinadas nos depoimentos, interrogatórios, denúncias e entrevistas com colaboradores e informantes. As fontes de conteúdo podem ser exemplificadas com os registros provenientes de sistemas bancários, ocorrências policiais, notícias da mídia, bem como de documentos de toda ordem. Já as fontes tecnológicas têm sua expressão na telecomunicação, imagens e sinais eventualmente interceptados, captados e devidamente analisados (BARTH *et al*., 2007), sendo esta última o foco principal deste estudo.

Obviamente, o serviço de segurança pública e o sistema de investigação incluem o rol dos ramos onde a presença do *big data* é relevante, principalmente com as enormes quantidades de informações oriundas de fontes tecnológicas disponíveis no cotidiano (redes sociais, comunicações instantâneas, aplicativos diversos, transmissão de áudio e vídeo em tempo real). Tal fato vem se consolidando há alguns anos, com o uso de medidas cautelares de quebra de sigilo de dados telemáticos para obtenção de provas no âmbito da persecução criminal. Neste ponto, para o desenvolvimento da investigação, o Código de Processo Penal (BRASIL, 1941) prevê diversas diligências que podem ser realizadas na sua fase instrutória, as quais podemos dividir entre ordinárias e extraordinárias.

As diligências ordinárias estão previstas nos artigos 6° e 7° do CPP, que estabelecem várias possibilidades, exame legal de crime; apreensão de provas destinadas aos esclarecimentos do fato e suas circunstâncias; oitiva do ofendido, testemunhas e indiciado; reconhecimento de pessoas e coisas; acareação e diversas outras.

> Art. 6º - Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
>
> I - Dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)
>
> II - Apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)
>
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
>
> IV - Ouvir o ofendido;
>
> V - Ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura;
>
> VI - Proceder a reconhecimento de pessoas e coisas e a acareações;
>
> VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
>
> VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;
>
> IX - Averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter.
>
> X - Colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa. (Incluído pela Lei nº 13.257, de 2016)
>
> Art. 7o Para verificar a possibilidade de haver a infração sido praticada de determinado modo, a autoridade policial poderá proceder à reprodução simulada dos fatos, desde que esta não contrarie a moralidade ou a ordem pública. (BRASIL, 1941)

Nesta fase, é possível ainda realizar diligências extraordinárias como a representação por medidas cautelares sujeitas a reserva de jurisdição, tais como a quebra de sigilo bancário, fiscal, telefônico, telemático, bem como a interceptação telefônica, busca e apreensão, infiltração policial, colaboração premiada e ação controlada, entre outras. Assim, quando nos deparamos com a medida cautelar de quebra de sigilo telemático na investigação, temos enormes quantidades de informações digitais oriundas de fontes tecnológicas.

O conceito de utilização dos dados de fontes tecnológicas no cenário investigativo atual é quase condição *sine qua non* para o sucesso da investigação. Seria praticamente impossível, nesse universo de informações, a inexistência da transmissão de dados relativos aos ilícitos penais, como crimes financeiros, fraudes, corrupção, tráfico de drogas e diversos outros.

Atualmente, é fácil compreender o cenário tecnológico em que nos encontramos: recebemos e enviamos uma infinidade de mensagens em aplicativos de comunicação instantânea; dezenas de *e-mails* são trocados por dia; realizamos diversas transações bancárias a cada dia; operadoras de telefonia registram a todo instante chamadas; provedores de internet

permitem a transmissão de canais pessoais de áudio e vídeo em tempo real; espaços virtuais como o metaverso, onde as interações das pessoas podem ser multidimensionais, economia digital descentralizada, com o uso de moedas virtuais em jogos e investimentos financeiros; cadeias de suprimentos virtuais registradas em *Blockchain*; equipamento e utensílios domésticos conectados à internet formando a internet das coisas e dezenas de outros cenários de tecnologias disruptivas que vêm compondo a transformação digital desta década.

Assim, não faltam exemplos para se observar o crescente volume de tráfego de informações ao redor do mundo, implicando um aumento cada vez maior de arquivos oriundos das fontes tecnológicas. Este novo mundo informacional vem ampliar o horizonte da investigação, quando nos deparamos com a existência das demais fontes de dados tradicionais, como registros policiais, banco de dados de registros civis, materiais apreendidos em operações policiais (SAISSE, 2017). Em função dessa nova realidade, surge a necessidade de repensar nos métodos de gestão, organização, tratamento e armazenamento desses arquivos para uma recuperação inteligente da informação em uma investigação policial. Neste ambiente digital tão vasto e de rápida evolução, também surgiram as tecnologias disruptivas, termo que descreve uma inovação tecnológica, como por exemplo a tecnologia *Blockchain* e o armazenamento digital distribuído em nuvem.

2.1.3 Armazenamento tradicional e em nuvem

A Evolução Tecnológica é algo que sempre esteve presente na vida da sociedade e ela evolui constantemente; a capacidade de processar dados aumentou exponencialmente com o tempo. Diante disso, os meios de armazenamento de dados precisam acompanhar essa evolução.

Na década de 60-70, os *floppy disks*, ou disquetes, foram lançados no mercado com a finalidade de gravar dados; eles possuíam a capacidade de armazenar apenas 1.44 MB. Felizmente, os avanços não pararam e discos rígidos, CDs, CD-Rs, CD-RWs, DVDs, *Blu-ray Discs*, HDs, SSDs e cartões de memória surgiram nos anos seguintes. Nos tempos atuais, entre *pen-drives*, plataformas móveis, servidores físicos e na nuvem, existem diversas alternativas (GODA, 2012).

O armazenamento de dados trata, basicamente, das ferramentas e dos métodos que são usados para guardar, catalogar e acessar os arquivos digitais; são fonte de informações a serem recuperadas conforme a necessidade, permitindo ainda manter essa informação preservada para uso futuro. A principal intenção do armazenamento é garantir que será possível o acesso a esses dados posteriormente, independentemente de qualquer problema de funcionamento ou interrupção na estrutura do processamento ou do armazenamento e em sua proteção contra possíveis ataques cibernéticos. Implica a garantia dos pilares da segurança da informação, confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade.

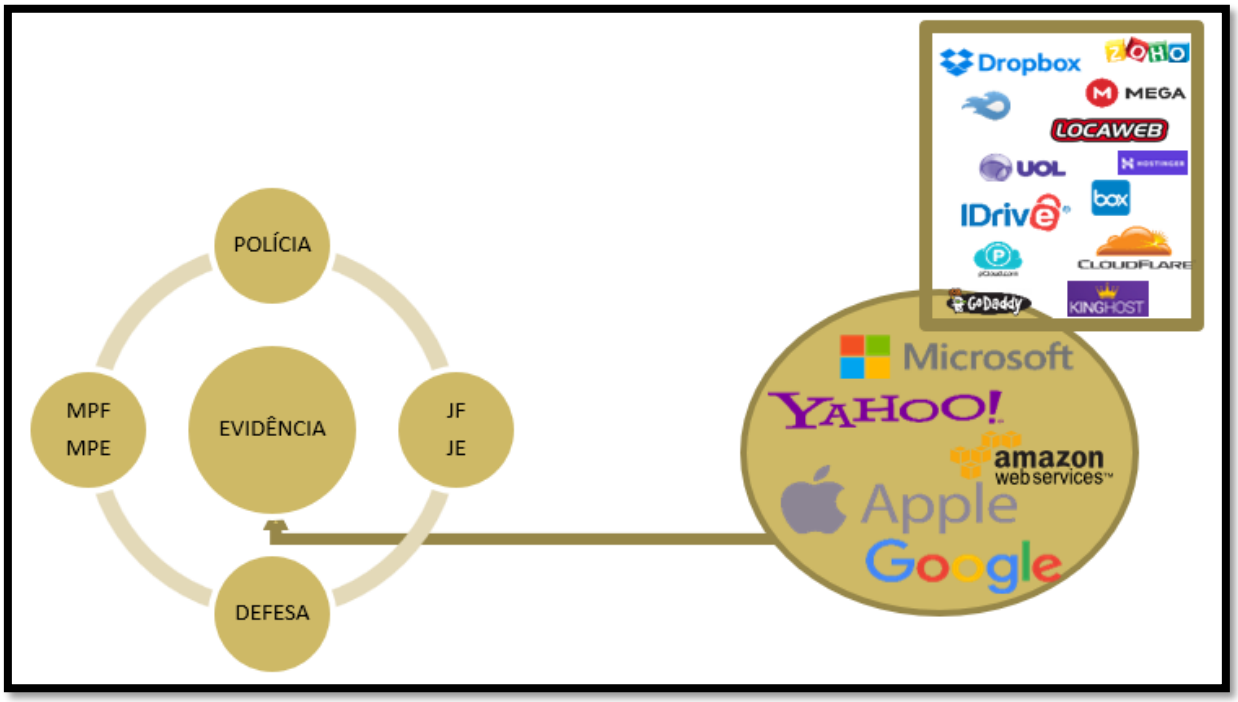
Destacam-se, basicamente, três tipos de armazenamento de dados de computador: armazenamento óptico, armazenamento magnético e em memórias *flash* (armazenamento eletrônico). E quanto à localização, podem ser armazenamentos locais ou localizados em nuvem (*cloud storage*).

Em seu artigo, Goda (2012) descreve os contextos recentes de computação em nuvem, o armazenamento remoto. Serviços que costumavam ser chamados de SSPs (*Storage Service Providers*) são frequentemente fornecidos como parte de serviços completos de nuvem. Atualmente, os principais serviços de armazenamento baseados em nuvem incluem *Amazon S3, Windows Azure Storage e Google Cloud Storage*, todos projetados em estreita coordenação com seus outros serviços de nuvem. O armazenamento baseado em nuvem não se limita a sistemas corporativos e está se tornando mais popular para novos tipos de consumidor eletrônico, como reprodutores de áudio/visual digital e leitores de livros. *Apple iCloud* e *Amazon Cloud* são importantes serviços que permitem aos clientes armazenar e gerenciar seus conteúdos comprados em nuvens remotas. A computação em nuvem é uma tecnologia emergente e atualmente bem difundida.

Sendo assim, os *smartphones* e seus aplicativos e a Internet das Coisas funcionam sobre dois grandes pilares: o armazenamento em nuvem e a coleta de dados pessoais de seus usuários. Esse universo digital não está isento de criminalidade; nestes armazenamentos, encontram-se possíveis evidências criminais. E as grandes empresas fornecedoras desses serviços serão requisitadas pela justiça pelo afastamento de sigilo dos dados quando necessário.

Na imagem a seguir (Figura 4), ilustramos a produção da Evidência Digital como centro do processo, produzidas pelas grandes empresas de tecnologia majoritárias do mercado (Google, Apple, Microsoft, Amazon) e diversas outras empresas minoritárias, em seu entorno, estão os atores da persecução criminal Justiça, Polícia, Ministério Público e Defesa.

Figura 5 - Investigação Criminal e as Fontes Tecnológicas



Fonte: Elaborado pelo autor (2022)

2.2 A CADEIA DE CUSTÓDIA E OS DADOS ARMAZENADOS EM NUVEM

Como bem explicado por Jorge (2021), a necessidade de produção de conhecimento de forma mais rápida levou o trabalho policial a fazer uso das informações produzidas através dessas tecnologias disruptivas, como forma de otimizar os resultados dentro da investigação. Nesse ambiente, órgãos de segurança pública identificaram novas possibilidades de afastamento de sigilo junto a empresas de tecnologia.

Ainda conforme o autor, a legislação brasileira permite avançar neste sentido, a partir do momento em que é permitido o afastamento do sigilo de registros de acessos e aplicações de internet. Dentre a legislação referente à requisição de dados cadastrais, podemos citar as seguintes leis: Lei do Marco Civil da Internet (Art. 10, 5 3º da Lei 12.965/2014); Lei de Lavagem de Capitais (art. 17-B da Lei 9.613/98); Lei de Crime Organizado (art. 15 da Lei 12.850/13); Lei de Investigação Criminal (art. 2º, § 2º da Lei12.830/13); e Nova Lei do Tráfico de Pessoas (Lei 13.344/2016).

A Lei do Marco Civil da Internet (Lei 12.965/14), ainda com mais propriedade, é utilizada para subsidiar a medida cautelar de afastamento de sigilo de Registro de Acesso e

Aplicações de Internet. Em sua maioria, são dados armazenados em nuvem[8]. Desta forma, com o afastamento do sigilo, o fornecimento de dados trará um novo horizonte de informações para a investigação, possibilitando o deslindamento de delitos que antes da persecução criminal tradicional muitas vezes duravam anos ou jamais subsidiaram a conclusão de autoria.

Entretanto, surgiu a preocupação com a produção das provas tecnológicas no processo penal, de forma especial com aquelas produzidas fora do processo. Procedimentos precisam ser adotados com a finalidade de garantir a imutabilidade da prova, ou seja, afastar qualquer possibilidade de arguição de manipulação ou adulteração de seu conteúdo.

O Código de Processo Penal (Decreto-Lei nº 3.689, de 3 de outubro de 1941) foi atualizado pela Lei nº 13.964, de 24 de dezembro de 2019, conhecido como "pacote anticrime", aperfeiçoando a legislação penal e processual penal e em especifico o capítulo II, "Do exame de corpo de delito, da cadeia de custódia e das perícias em geral", e deixou claro, quanto ao trato do vestígio criminal e sua cadeia de custódia.

> Art. 158-A considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.
>
> Art. 158-F. Após a realização da perícia, o material deverá ser devolvido à central de custódia, devendo nela permanecer. (BRASIL, 2019).

Apesar da recente atualização da legislação de dezembro de 2019, a lei se omite em relação às evidências virtuais ou armazenadas em equipamentos eletrônicos e quiçá em armazenamento em nuvem. O legislador trata apenas dos vestígios dos crimes "tradicionais", como os físicos e palpáveis, e assim perde a chance de regulamentar adequadamente a cadeia de custódia de crimes eletrônicos (JORGE, 2021).

Assim, chegamos ao ponto de questionar como preservar a cadeia de custódia dos dados fornecidos pelas empresas de armazenamento em nuvem. Inicialmente, a fim de manter a cadeia de custódia íntegra, o procedimento adotado pelos profissionais forenses segue o Padrão de Perícia Criminal e da Portaria nº 84/2014, ambas do Ministério da Justiça. Os fundamentos desses procedimentos forenses são originários de quatro fontes primárias: o Código Processual Penal Brasileiro, em seu art. 158-B, norma ABNT NBR ISO/IEC

[8] O armazenamento em nuvem é um modelo de computação em nuvem que permite armazenar dados e arquivos na Internet por meio de um provedor de computação em nuvem que você acessa usando a Internet pública ou uma conexão de rede privada dedicada. O provedor armazena, gerencia e mantém com segurança os servidores de armazenamento, a infraestrutura e a rede para garantir que o acesso aos dados onde e quando o usuário precisar, em escala praticamente ilimitada e com capacidade elástica. Fonte: Amazon Web Services - https://aws.amazon.com/pt/what-is/cloud-storage/#seo-faq-pairs#what-is-cloud-storage.

27037:2013; o RFC[9] 3227 – *Guidelines for Evidence Collection and Archiving*; e a partir da publicação do documento *Special Publication* 800-86 do National Institute of Standards and Technology (NIST).[10]

Em um segundo momento, para afastar qualquer alegação de manipulação ou adulteração dos dados obtidos, a autoridade policial deve representar ao Judiciário, para que as empresas de armazenamento, além de fornecerem o material para *download*, encaminhem uma cópia idêntica em mídia física a ser juntada na medida cautelar. Isto seria um meio ideal para manutenção da cadeia de custódia e observância aos princípios do contraditório e da ampla defesa. No entanto, ambas as situações descritas acima possuem falhas.

Na maior parte do cotidiano da investigação policial, o processo de aquisição e análise dos dados armazenados em nuvem fica a cargo do policial, e não do profissional forense, o que abre a possibilidade da inobservância dos protocolos forenses. Existe ainda a dificuldade de as empresas encaminharem a cópia em mídia física dos dados requisitados, por questões técnicas e de alta demanda; então o fazem disponibilizando os dados por meio de *downloads* em seus portais *web* de acesso restrito.

2.2.1 Cadeia de custódia e *blockchain*

De acordo com Santos (2019), a tecnologia *Blockchain* é uma espécie de banco de dados distribuído projetado para processar e armazenar informações. E embora a maioria das implementações *Blockchain* da atualidade sejam utilizadas em operações financeiras, tais infraestruturas servem para armazenar informações diversas, como por exemplo, carimbos de tempo (*timestamp*) de documentos com vistas a proteger sua integridade. Em se tratando de privilégios de acesso, às *Blockchains* podem ser classificadas em públicas e privadas.

Ainda conforme o trabalho do autor, por definições de projeto, *Blockchains* são inerentemente resistentes à modificação não autorizada de seus dados. Uma vez gravados, os dados em qualquer bloco não podem ser alterados retroativamente sem a alteração de todos os

[9] A *Request for Comments* (RFC) é uma publicação de uma série dos principais organismos de desenvolvimento técnico e de normalização da Internet, com destaque para o Internet Engineering Task Force (IETF). RFC 3227 em Português – *Guidelines for Evidence Collection and Archiving*. Disponível em: https://tools.ietf.org/html/rfc3227. Acesso em: 07 ago. 2021.
[10] National Institute of Standards and Technology. *Guide to integrating forensic techniques into incident response*. NIST Special Publication 800-86. Gaithersburg: NIST, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Acesso em: 07 ago. 2021.

blocos subsequentes e a validação de toda a rede de blocos interligados. Em termos funcionais, uma cadeia de blocos pode servir como um "livro-razão" (*ledger*) aberto e distribuído, que pode gravar as transações entre duas partes de forma eficiente e de forma verificável e permanente.

Generalizando um pouco o conceito para livro de registros, é possível realizar o acompanhamento de outros tipos de informação, como: as operações de compra, venda ou hipoteca de imóveis ou terras; as medicações, exames e procedimentos aplicados a um paciente internado no hospital; e muitas outras mais (ARANTES JUNIOR, 2018).

Um dos maiores desafios na cadeia de custódia é manter a integridade dos dados. Uma falha de segurança no manuseio dessas evidências põe em risco todo o processo criminal. De acordo com Bonomi *et al*. (2018), a cadeia de custódia é o processo de validação de como qualquer tipo de evidência foi recolhida, rastreada e protegida no caminho até o Judiciário. A evidência digital é parte integrante do processo de investigação. Assim, no processo judicial também, as evidências desempenham importante papel. A principal razão que nos leva a interagir com a tecnologia *Blockchain* é a possibilidade de se criar um livro-razão completo de todas essas interações com a evidência digital de forma segura e inalterável. O ordenamento jurídico brasileiro no Código de Processo Penal (Decreto-Lei nº 3.689, de 3 de outubro de 1941) é claro quanto ao trato do vestígio criminal e sua cadeia de custódia.

É de extrema importância garantir integridade, autenticidade e auditoria de evidências digitais à medida que se move em diferentes níveis de hierarquia, ou seja, dos investigadores que obtêm a prova, até as autoridades do Judiciário, responsáveis por lidar com a investigação e com as instâncias de defesa do acusado. O principal problema na cadeia de custódia é a documentação e registro da interação com a evidência; quando esta é usada por múltiplas partes, já se associa um risco de adulteração.

A capacidade da tecnologia *Blockchain* de se dividir em diversos registros que permitem um abrangente rastreamento das informações atreladas àqueles registros desde sua origem, abre uma monumental possibilidade para a comunidade forense, permitindo o registro de movimentação de uma evidência em toda a sua cadeia de custódia, do começo ao fim. Basicamente, uma informação distribuída mantém uma estrutura à prova de adulteração incessantemente crescente em seus diversos blocos de transações individuais, implementando um livro-razão descentralizado e totalmente replicado em uma rede *peer-to-peer* (GOPALAN, 2019).

2.3 BLOCKCHAIN

Blockchain é um sistema de livros-razão *peer-to-peer*[11] puramente distribuído que utiliza uma unidade de *software* que consiste em um algoritmo, que negocia o conteúdo informacional de blocos de dados ordenados e conectados junto com tecnologias criptográficas e de segurança para alcançar e manter sua integridade (KUBE, 2017).

2.3.1 Conceito

Em uma definição mais simples, *Blockchain* é um registro descentralizado e distribuído de informações que é controlado e atualizado por uma comunidade de usuários. Não existe uma entidade ou pessoa central que controle o registro.

De acordo com Don Tapscott (2014), o *Blockchain* é um livro digital incorruptível de transações econômicas que pode ser programado para registrar não apenas transações financeiras, mas praticamente tudo de valor. Ainda segundo o autor, *Blockchain*s são como livros-razão distribuídos para revolucionar a forma como a informação é armazenada e as transações ocorrem. Seus objetivos são louváveis: velocidade, menor custo, segurança, menos erros e a eliminação de pontos centrais de ataque e falha.

Na origem da *Blockchain,* está o protocolo do *Bitcoin*, proposto por Satoshi Nakamoto (NAKAMOTO, 2008), que entrou em operação em 2009. O artigo seminal propõe uma rede puramente *peer-to-peer* de dinheiro eletrônico que permitiria que pagamentos *on-line* fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira. No sistema de rede descentralizado e distribuído, as transações propostas por clientes (nós) são recebidas por servidores (mineradores), que irão decidir, através de um protocolo de consenso à base de desafios criptográficos, a ordem em que elas serão realizadas e armazenadas permanentemente numa corrente de blocos (*Blockchain*) replicada em cada servidor.

Importante notar que a *Blockchain* do *Bitcoin* proposta por Nakamoto só possibilita transações monetárias. Desta forma, não havia como adicionar condições mais elaboradas a essas transações. Em 2013, Vitalik Buterin propôs uma plataforma para o desenvolvimento de

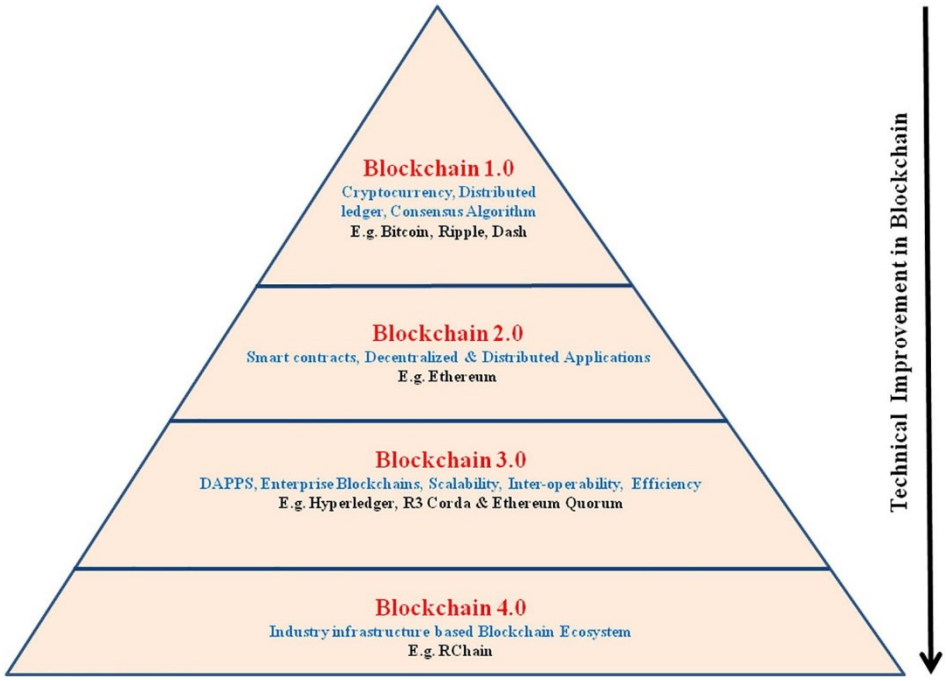
[11] *Peer-To-Peer* - arquitetura de redes de computadores em que cada um dos pontos ou nós da rede funcionam tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

aplicações descentralizadas chamada *Ethereum*. Com o suporte para contratos inteligentes (em inglês, *smart contracts*), elevou-se a um novo patamar a tecnologia *Blockchain,* uma vez que esta permitiu executar, de forma autônoma e confiável, um código (ou programa) acordado previamente por duas ou mais partes (BRASIL-TCU, 2018).

> **Consenso** em uma rede refere-se ao processo de obtenção de um acordo entre os participantes da rede quanto ao estado correto dos dados no sistema. O consenso leva a todos nós compartilhando exatamente os mesmos dados. Portanto, um algoritmo de consenso (i) garante que os dados no livro-razão sejam os o mesmo para todos os nós da rede e (ii) evita ataques maliciosos atores de manipular os dados. [...]
>
> ***Smart contract*** – contrato inteligente é um programa de computador que executa ações predefinidas quando certas condições dentro do sistema são atendidas. Os contratos inteligentes fornecem o idioma das transações, permitindo que o estado do livro-razão seja modificado. Eles podem facilitar a troca e transferência de qualquer ativo (por exemplo, ações, moeda, conteúdo, propriedade). eles residem na estrutura do *Blockchain* e são acionados junto com transações. Contratos inteligentes podem ser imaginados como protocolos digitais usados para facilitar e reforçar a negociação de um contrato legal. Ações realizadas por pessoas de confiança terceiros durante uma negociação são substituídos por pedaços de código. [...]
>
> ***Ethereum*** é uma rede aberta plataforma projetada para construir e usar aplicativos descentralizados que executam contratos inteligentes, ou seja, uma rede *Blockchain* de aplicativos distribuídos que executam tarefas mecanicamente quando certas condições são atendidas. Isso pode ser feito em um grau maior do que o possível com o modelo *Bitcoin*. (BELOTTI *et al*., 2019, tradução e grifo nossos)

A *Blockchain* evoluiu conforme os recursos tecnológicos e aprimoramentos na rede e nas aplicações às quais se destinava. Tal evolução resultou em diversas gerações da tecnologia, melhorando entre suas gerações 1.0 até 4.0, o que tornou a tecnologia mais adequada para aplicações nas mais diversas áreas. Mais escalável, programável, com uma estrutura de dados otimizada para blocos e transações, novos métodos de consenso geraram uma enorme demanda de *Blockchain* em todos os aplicativos do mundo real. A figura abaixo mostra a evolução dessa tecnologia.

Figura 6 - Evolução da *Blockchain*



Fonte: SHRIMALI *et al*., 2022

Conforme pode ser observado na Figura 5, na primeira geração, a *Blockchain* (1.0) foi limitada a armazenar e transferir valor (principalmente em criptomoedas, por exemplo, *Bitcoin, Ripple, Dash*).[12] Em sua segunda geração, o ambiente da *Blockchain* (2.0) passou a ser programável via contratos inteligentes como *Ethereum* e Cardano,[13] e abriu as portas para aplicações descentralizadas e distribuídas. Já em sua terceira geração, *Blockchain* (3.0), a tecnologia tornou-se focada em aplicativos descentralizados (conhecido como DApps, deriva de *Decentralized Application*) que alcançam vida diária, facilitando vários setores, como saúde, educação, agricultura, *e-commerce* e muito mais. Exemplos desses *Blockchains* corporativos são *Hyperledger,*[14] R3 Corda[15] e *Ethereum Quorum.*[16] Em seguida, em sua quarta geração, *Blockchain* (4.0), foram removidas quase todas as limitações da *Blockchain* anterior. A rede *Blockchain* 4.0 passou a utilizar um sistema em ambiente distribuído, sofrendo grandes

[12] Criptomoedas que utilizam a tecnologia *Blockchain*.
[13] Plataforma de computação distribuída que executa o *Blockchain* para a criptomoeda ADA.
[14] Projeto colaborativo envolvendo várias indústrias, iniciado em dezembro de 2015 pela Linux Foundation. Tem como objetivo avançar a tecnologia de registro distribuído *Blockchain* em múltiplos segmentos da indústria.
[15] Consórcio entre diferentes empresas com o objetivo de implantar a *Blockchain* Corda na indústria e no mercado financeiro.
[16] *Quorum Blockchain Service* é um serviço de gestão gerenciado da ConsenSys. Ele permite que as organizações mantenham uma rede própria na *blockchain ethereum* sem precisar lidar com o gerenciamento de infraestrutura.

problemas com escalabilidade e limitação em transações por segundo. Isso levou a tecnologia a buscar avanços em infraestrutura para o aumento da estabilidade e velocidade. Exemplo disso é *RChain*, que espera ser uma plataforma para contratos inteligentes escalável, eficiente, confiável e verdadeiramente descentralizada, pretendendo uma arquitetura *Blockchain* correta para suportar a escalabilidade e a alta quantidade de transações por segundo (tps) necessárias para uso industrial. A tecnologia segue evoluindo para soluções de segunda camada[17] para resolver os problemas das gerações de *Blockchain* anteriores, além de outras soluções como as *Crosschains*, que possibilitam a conexão de diferentes *Blockchains*, permitindo a comunicação e verificação de dados e valores entre elas.

2.3.2 Principais elementos de uma *Blockchain*

Segundo a empresa IBM,[18] em sua divisão especializada em *Blockchain,* uma rede *Blockchain* tem as seguintes características principais: o Consenso, para que uma transação seja válida, todos os participantes devem concordar com a sua validade; a Proveniência, em que os participantes sabem de onde veio o ativo e como sua propriedade mudou ao longo do tempo; a Imutabilidade, porque nenhum participante pode adulterar uma transação depois de ter sido registrado no livro-razão. Se uma transação estiver em erro, uma nova transação deve ser usada para reverter o erro, e ambas as transações ficam visíveis; a Finalidade, pois um único livro-razão compartilhado fornece um lugar para onde ir, determinar a propriedade de um ativo ou a conclusão de uma transação.

2.3.3 Tipos de rede de *Blockchain*

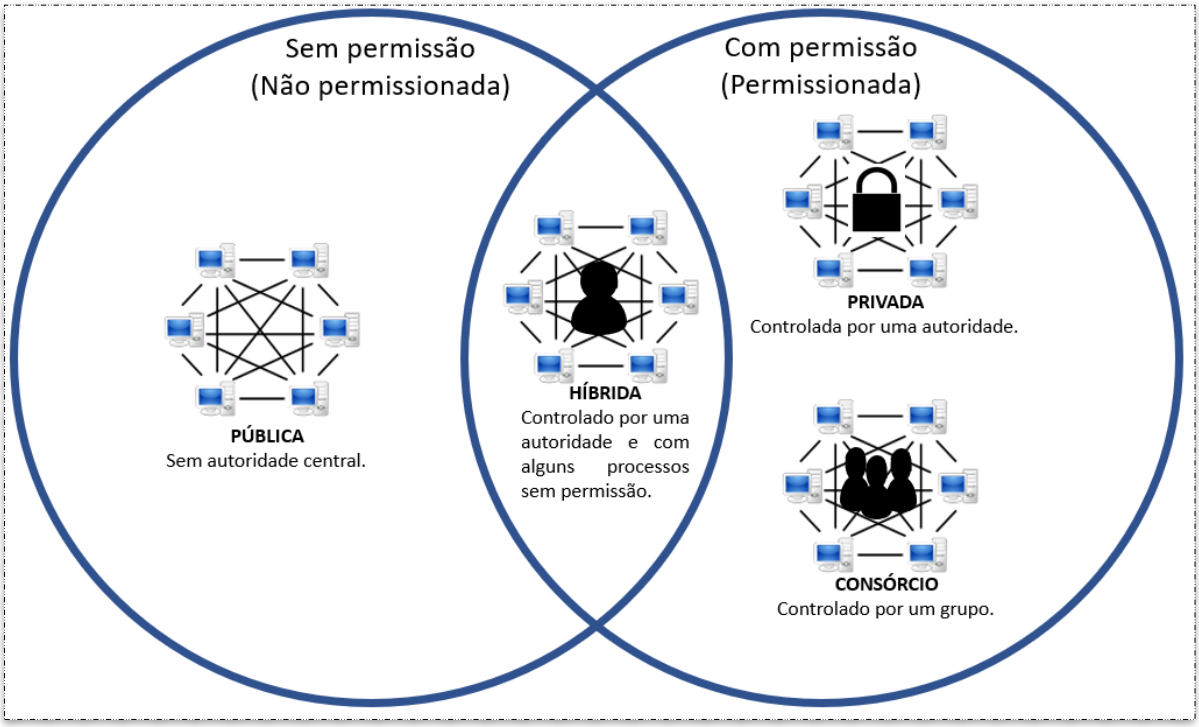
Em sua terceira edição, o manual *Blockchain for Dummies* (*Blockchain para leigos*) da empresa IBM, uma das pioneiras em projetos com *Blockchain* na iniciativa privada, apresenta essa tecnologia e descreve alguns conceitos. Segundo o manual, existem várias

[17] As redes de segunda camada são protocolos construídos em cima de uma *Blockchain* existente. O principal objetivo desses protocolos é aprimorar a velocidade de transações e reduzir os custos, problemas enfrentados pelas principais *Blockchains*.

[18] **IBM** – A *International Business Machines Corporation* é uma empresa dos Estados Unidos voltada para a área de informática. A empresa IBM Blockchain está levando o mundo dos negócios a uma nova era de colaboração e inovação. A IBM Blockchain funciona graças à ajuda de mais de 1.600 especialistas em negócios e técnicos da IBM que trabalham em mais de 500 projetos atualmente. Fonte: https://www.ibm.com/br-pt/blockchain

formas de se criar uma rede *Blockchain.* Essas redes podem ser públicas, privadas, híbridas ou desenvolvidas por um consórcio (federadas).

Figura 7 - Tipos de *Blockchain*



Fonte: Adaptado de https://www.simplilearn.com/

A Figura 6, acima, representa a interseção dos tipos de tecnologias *Blockchain* sob a característica de permissionamento. É possível verificar que a rede híbrida possui características mistas de permissão (escrita e leitura do livro-razão); a rede privada e de consórcio são totalmente permissionadas; e a única sem permissão é a rede pública.

a. Redes de *Blockchain* públicas

Em uma *Blockchain* pública, qualquer pessoa pode entrar e participar. O *Bitcoin* é um exemplo desse tipo de rede. As desvantagens podem incluir uso excessivo de computadores, pouca ou nenhuma privacidade nas transações e segurança fraca. Essas são considerações importantes nos casos de uso empresarial da *Blockchain.*

- *Blockchains* públicas permitem que qualquer pessoa faça parte delas. Seja como usuário, minerador ou administrador de um nó, as pessoas podem acessar a rede e fazer parte dela sem qualquer restrição.
- O funcionamento da rede é totalmente transparente e aberto. Os dados da *Blockchain*, desde seu início, estão disponíveis para todos sem restrições. Qualquer pessoa pode revisar ou auditar a operação da rede e seu *software.*
- Não existem entidades centralizadas. As redes públicas são totalmente descentralizadas e não existe uma autoridade central que regula seu funcionamento.
- A manutenção econômica da *Blockchain* depende do sistema integrado a ela. Geralmente, esse sistema econômico depende da mineração e da cobrança de comissões por cada transação realizada dentro da rede.

b. Redes de *Blockchain* privadas

Uma *Blockchain* privada é uma rede ponto a ponto descentralizada como a *Blockchain* pública. No entanto, uma empresa administra a rede e controla quem pode participar, executar um protocolo definido e manter o livro-razão compartilhado. Dependendo do caso de uso, isso pode aumentar consideravelmente a confiança e a segurança dos participantes.

- O acesso à rede é restrito a itens que só podem ser autorizados pela unidade de controle central.
- O acesso ao livro de transações ou qualquer outro meio de informação gerado pelo *Blockchain* é privado.
- A manutenção econômica da *Blockchain* geralmente depende da empresa que apoia o projeto. Frequentemente, *Blockchains* privadas não possuem criptomoedas ou ações de mineração.
- Embora tenha uma conexão ponto a ponto semelhante e descentralização para uma rede *Blockchain* pública, a *Blockchain* é muito menor.
- Geralmente são executadas em uma pequena rede dentro de uma empresa ou organização, em vez de serem abertas a qualquer pessoa que queira contribuir com poder de processamento.

c. Redes de Blockchain híbridas

Uma Blockchain que combina elementos de Blockchain pública e privada, permitindo que as organizações configurem um sistema privado baseado em permissão junto com um sistema público sem permissão. Isso permite que se controle quem pode acessar dados específicos armazenados na Blockchain e quais dados serão abertos publicamente. Isso restringe as transações e quem pode participar da rede. As pessoas precisam receber um convite ou ter permissão para participar. Apesar de as informações confidenciais serem mantidas dentro da rede, ainda podem ser verificadas. Então, mesmo que uma entidade privada possa possuir a Blockchain híbrida, ela não pode alterar as transações.

- O acesso à rede está restrito a itens que só podem ser autorizados pelas demais unidades de controle.
- O acesso ao livro de transações ou qualquer outro meio de informação gerado pelo *Blockchain* é público.
- Não há mineração ou criptomoedas. O consenso da rede é dado por outros meios que garantem que os dados estejam corretos.
- É parcialmente descentralizada, o que leva a um melhor nível de segurança e transparência.
- Em uma *Blockchain* híbrida, transações e registros normalmente não são públicos, mas podem ser validados, se necessário, concedendo acesso por meio de um contrato inteligente.

d. *Blockchain* de consórcio

Uma rede Blockchain de consórcio é controlada por um conjunto de organizações ou nós pré-selecionados, em vez de um nó centralizado ou uma rede descentralizada. Várias empresas podem compartilhar as responsabilidades de manutenção de uma *Blockchain.* Essas empresas pré-selecionadas determinam quem pode enviar transações ou acessar dados.

- Da mesma forma que uma *Blockchain* híbrida possui recursos de *Blockchain* privadas e públicas, uma *Blockchain* de consórcio, também conhecida como *Blockchain* federada, possui.

- Envolve vários membros organizacionais, trabalhando juntos em uma rede descentralizada.
- Nós predeterminados controlam os métodos de consenso em um *Blockchain* de consórcio.
- Possui um nó validador responsável por iniciar, receber e validar transações. As transações podem ser iniciadas ou recebidas por seus membros.
- Uma *Blockchain* de consórcio é mais segura, escalável e eficiente do que uma rede pública de *Blockchain*.

Quadro 1 - Resumo dos tipos de Blockchain

Tipos de *Blockchain*	**Rede Aberta**	**PÚBLICA**	Livro-razão aberto Com mineração Validação de blocos sem permissão	Qualquer pessoa pode entrar e participar do consenso.	Sistema de livro-razão aberto totalmente descentralizado, seguro e imutável.	As transações são anônimas, mas transparentes para todos
	Rede Fechada	**PRIVADA**	Livro-razão fechado Sem mineração Validação de blocos com permissão	Uma única organização terá autoridade sobre a rede.	Saída mais rápida, eficiência de energia e oferece privacidade.	Processo de manipulação de dados simplificado, mas não aberto a todos.
		HÍBRIDA	Livro-razão fechado ao público aberto aos membros Sem mineração Validação de blocos com permissão	Acesso autoritativo, apenas alguns elementos são privados	Controle flexível sobre quais dados são mantidos públicos e privados	Sistema descentralizado, regulado e altamente escalável.
		CONSÓRCIO	Livro-razão aberto entre membros Sem mineração Validação de blocos com permissão	Múltiplas organizações influenciam a rede blockchain.	Sistema descentralizado, extremamente rápido e escalável.	Os regulamentos de rede preservam a segurança e a privacidade.

Fonte: SANTOS *et al*., 2019 e Adaptado e traduzido de https://101blockchains.com/types-of-blockchain

O quadro acima resume as principais características e diferenças entre os tipos de *Blockchains*.

2.3.4 Dificuldades e problemas no uso de *Blockchain*

Os trabalhos aqui estudados apontam suas especificidades em relação às dificuldades de suas propostas, em sua maioria relacionadas a questões de escalabilidade e segurança. De forma geral, os principais elementos que trazem problemas à tecnologia são resumidos a seguir.

- A rede pode ser lenta e as empresas não podem restringir o acesso ou uso. Portanto, se os *hackers* obtiverem 51% ou mais do poder de computação de uma rede pública de *Blockchain*, eles podem alterá-la unilateralmente (*Blockchain* pública).
- As desvantagens das *Blockchains* privadas incluem a alegação controversa de que elas não são verdadeiras *Blockchains*, uma vez que a filosofia central da *Blockchain* é a descentralização. Não obstante, também é mais difícil obter confiança total nas informações. Afinal, são os nós centralizados que determinam o que é válido. Então, o pequeno número de nós também pode significar menos segurança, porque o método de consenso é comprometido caso alguns nós falhem. Além disso, o código-fonte da *Blockchain* privada é geralmente proprietário e fechado. Portanto, os usuários não podem auditar ou confirmar de forma independente, o que pode levar a menos segurança. Também não há anonimato (*Blockchain* privada).
- As informações podem ser protegidas; então, este tipo de *Blockchain* não é completamente transparente. Atualizar também pode ser um desafio, e não há incentivo para os usuários participarem e contribuírem com a rede (*Blockchain* híbrida).
- A *Blockchain* do consórcio é menos transparente do que a *Blockchain* pública. Além disso, ao se violar um nó, ele ainda pode ser comprometido. Portanto, os próprios regulamentos da *Blockchain* podem prejudicar a funcionalidade da rede (*Blockchain* consórcio).

O TCU (BRASIL-TCU, 2018) elaborou um guia sobre uso de *Blockchain* no serviço público, em que diversos exemplos em uso ou desenvolvimento são apresentados. Neste trabalho, em seu Apêndice 2, é apresentada uma matriz de riscos do uso da tecnologia *Blockchain* no cenário nacional; descrevem-se ainda os principais pontos que podem convergir com a proposta desta pesquisa.

No levantamento de riscos realizados pelo TCU, foram descritos os riscos específicos, principalmente para uma *Blockchain* de consórcio, os controles possíveis e os critérios

utilizados, com base no COBIT[19] BAI02 – *Managed Requirements Definition*, no COBIT BAI03 – *Managed Solutions Identification and Build* e na IN SGD[20] 1/2019, art. 16, incisos I e II. Em todos os riscos descritos, foram apontados diversos controles possíveis.

A seguir, são descritos alguns dos principais e relevantes riscos específicos e possíveis controles.

1) Funcionamento e desempenho da rede

- Risco: Não satisfação dos requisitos da aplicação pelo algoritmo de consenso escolhido.

  Solução: Garantir que todos os requisitos das partes interessadas sejam identificados, priorizados e registrados, com a finalidade de validar se o algoritmo de consenso escolhido atende às necessidades dos diferentes participantes da rede. Identificar qual é a topologia de rede do sistema e verificar se os nós que poderão participar do consenso são confiáveis ou não e se a organização ou o consórcio possui a quantidade suficiente de nós para executar o protocolo de consenso. Entender o funcionamento, os incentivos, as vantagens e desvantagens de cada um dos algoritmos de consenso disponíveis para uso pela plataforma utilizada.

- Risco: Dimensionamento incorreto dos requisitos de escalabilidade e desempenho.

  Solução: Contabilizar a quantidade de nós e as transações por segundo (tps) esperadas pela aplicação; identificar as necessidades referentes à taxa de transferência (*throughput*) e ao intervalo de transmissão à rede de transações, incluindo tempo máximo e médio de uma transação; verificar se o tamanho e o formato do bloco são compatíveis com as necessidades da aplicação e suportados pela plataforma utilizada.

- Risco: Definição incorreta dos direitos de acesso ao livro-razão.

---

[19] **COBIT** – Controle de Objetivos para Informação e Tecnologias Relacionadas mais conhecido pela abreviação COBIT, é um guia ou conjunto de boas práticas sobre governança de tecnologia de informação empresarial, criado em 1996 pela ISACA, para gerenciamento dos recursos e ferramentas tecnológicas da empresa.
- BAI02 Realizar um estudo de viabilidade e formular soluções alternativas.
- BAI03 Gerenciar o risco de requisitos.

[20] **IN SGD** – Instrução Normativa da Secretaria de Governo Digital, norma do governo que dispõe sobre o processo de contratação de soluções de tecnologia da informação e comunicação, pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação, do Poder Executivo Federal.

Solução: Definir quem são os nós validadores da rede (*commit*), ou seja, quem participa do mecanismo de consenso; identificar quais são os tipos de transações, quem pode realizar essas transações (*write*), bem como quem pode visualizar (*read*) e auditar os dados da *Blockchain*.

2) Integração e interoperabilidade

- Risco: Problemas de desempenho e integração com sistemas *off-chain*.
- Solução: Identificar e mensurar o impacto da aplicação *Blockchain*/DLT [21]nos sistemas existentes, como por exemplo, a necessidade de desenvolvimento de adaptadores de acesso; verificar se a plataforma *Blockchain*/DLT utilizada tem capacidade de se comunicar com outros sistemas externos: interfaces de usuário, gerenciamento de chaves criptográficas, integração da internet das coisas e de bancos de dados; definir estratégia de realização de testes de integração com sistemas existentes.
- Risco: Incompatibilidade entre diferentes redes *Blockchain* (*Hyperledger*, Corda, *Quorum, Ethereum* etc.).
- Solução: Identificar os mecanismos disponíveis de interoperabilidade entre plataformas; verificar se o sistema DLT deve ter APIs[22] padronizadas, como serviços de acesso, dicionário de dados, protocolo de comunicação, algoritmo de criptografia e teste do sistema, para que possa haver fornecedores que ofereçam serviços compatíveis;

3) Construção, implantação, suporte e manutenção da rede

- Risco: Abandono de suporte da plataforma *Blockchain* pelo fabricante ou consórcio de empresas responsáveis pelo desenvolvimento, pela evolução e pela manutenção do projeto.

[21] *Distributed Ledger Technology* ou Tecnologia de Ledger Distribuído - é um banco de dados (livro-razão) digital composto de informações copiadas, compartilhadas e sincronizadas.
[22] API significa *Application Programming Interface* (Interface de Programação de Aplicação). No contexto de APIs, a palavra Aplicação refere-se a qualquer software com uma função distinta. A interface pode ser pensada como um contrato de serviço entre duas aplicações.

Solução: Acompanhar os repositórios de desenvolvimento (*SLACK*[23] e *GITHub*[24]). O acompanhamento deve ser feito pelos profissionais da organização; avaliar o nível de utilização e dominância de mercado da plataforma *Blockchain* escolhida.

- Risco: Falha ou interrupção do projeto *Blockchain*/DLT da organização. Solução: Avaliar a possibilidade de se adotar plataformas de código aberto e conduzir projeto-piloto com escopo reduzido para validar o caso de uso e os requisitos de negócio.

- Risco: Escolha inadequada da plataforma *Blockchain*/DLT a ser utilizada pela organização ou pelo consórcio.

  Solução: Definir os requisitos funcionais e não funcionais relacionados ao caso de uso; entender os objetivos de *design*, a finalidade e a forma de funcionamento das plataformas disponíveis; comparar diferentes plataformas, com base na análise e avaliação das funcionalidades de cada uma.

- Risco: Imaturidade das redes e plataformas de *Blockchain/DLT* existentes.

  Solução: Avaliar a possibilidade de utilizar outras soluções, tais como banco de dados distribuídos e *APIs REST;*[25] verificar a possibilidade de implementar uma camada de abstração para acesso aos recursos da plataforma nativa de *Blockchain*; aguardar e monitorar evoluções tecnológicas que possam apoiar ou impactar o alcance dos objetivos de negócios.

4) Desenvolvimento de código e execução de aplicações

- Risco: Imprevisibilidade lógica do contrato inteligente.

  Solução: Identificar e validar condições de interrupção e término do contrato, para assegurar a resiliência do código; conduzir revisões e aceitação rigorosas de código, para garantir que o estado final dos dados na *Blockchain* seja entre os participantes, tanto para condições esperadas do negócio quanto para

[23] *Slack* é um programa de mensagens instantâneas desenvolvido pela Slack Technologies.
[24] *GitHub* é uma plataforma de hospedagem de código-fonte e arquivos com controle de versão usando o Git. Permite que programadores ou qualquer usuário cadastrado na plataforma contribuam em projetos privados e/ou Open Source de qualquer lugar do mundo.
[25] Na informática e engenharia de *software*, *Representational State Transfer*, em português Transferência de Estado Representacional é um estilo de arquitetura de *software*,

exceções; documentar as situações esperadas de sucesso e insucesso dos contratos inteligentes (requisitos de negócio) por meio de testes automatizados.

- Risco: Erros na escrita do código fonte dos contratos inteligentes, decorrentes de falhas no design do *software* e entendimento dos requisitos da aplicação. Solução: Definição de *design patterns*, boas práticas de desenvolvimento e geração automática de código, baseados em modelos testados*;* uso de ferramentas de análise de código e métodos formais de testes.

- Risco: Perda de transações enviadas à *Blockchain* que é acessada pela dApp.[26] O nó *Blockchain* que recebe a requisição do *frontend* a dApp pode estar indisponível, por ter tido o endereço trocado ou, simplesmente, o *software* do nó pode não executar a transação por algum motivo.

  Solução: Fornecer, nos *dApps*, *frontends* robustos que informem ao usuário a realização ou não de uma transação na *Blockchain*.

2.3.5 *Blockchain* e inovação disruptiva

O *Manual de Oslo* (OECD/Eurostat, 2018) é um documento que padroniza e preconiza elementos conceituais-chave da inovação no cenário mundial. Ele descreve como sendo os principais componentes do conceito de inovação: o papel do conhecimento como base para inovação; a novidade e utilidade; e a criação ou preservação de valor como objetivo presumido da inovação. A exigência de implementação é imperativa e diferencia inovação de outros conceitos como invenção, pois uma inovação deve ser implementada, ou seja, colocada em uso ou disponibilizada para uso de outros. Ainda de acordo com o manual, o termo "inovação" pode ser definido da seguinte forma:

> A inovação é um produto ou processo novo ou aprimorado (ou combinação deles) que difere significativamente dos produtos ou processos anteriores da unidade e que foi disponibilizado para usuários em potencial (produto) ou colocado em uso pela unidade (processo) (OECD/EUROSTAT, 2018, p. 246, tradução nossa).

Clayton Christensen (2019) cunhou um termo e conceito para um tipo de inovação, a "inovação disruptiva", que descreve um processo pelo qual inovações radicais são consideradas por transformar o *status quo*. Uma inovação disruptiva se enraíza em aplicações simples em um

[26] Aplicativos descentralizados (conhecido como DApps, deriva de *Decentralized Application*).

nicho de mercado e depois se difunde por todo o mercado; em seguida, incansavelmente sobe no mercado, eventualmente segregando concorrentes estabelecidos.

De outra forma, o autor entende que inovação disruptiva é aquela que permite a criação de um novo cenário de mercado, no qual os concorrentes que antes o dominavam acabam ficando deslocados, deixando obsoletos os antigos serviços ou produtos.

O sistema *Blockchain* nasceu por meio da proposta de uma moeda descentralizada, o *Bitcoin*, em um cenário econômico radical e disruptivo. A grande crise de 2008 criou um sistema financeiro instável e diversas medidas extremas e imprevistas empregadas pelas principais autoridades monetárias globais. Os motivos fundamentais que impulsionaram a criação do *Bitcoin* foram evidentes: um sistema financeiro instável e com elevado nível de intervenção estatal, e a crescente perda de privacidade financeira (ULRICH, 2014).

Blockchain é a mais recente "inovação disruptiva" que chamou a atenção dos estudiosos. É a tecnologia subjacente para *Bitcoin* e outras moedas digitais. Partes interessadas como desenvolvedores, empreendedores e entusiastas da tecnologia afirmam que o *Blockchain* tem o potencial de reconfigurar o cenário econômico, legal, político e cultural (FRIZZO-BARKER, 2020).

A tecnologia *Blockchain* estabeleceu uma maneira de digitalizar todas as nossas atividades através do desenvolvimento baseado em nuvem. Uma complexa tecnologia que incorporou uma visão engenhosa e poderosa para criar uma solução abrangente para a segurança da Internet. *Blockchain* está evoluindo rapidamente para ser a próxima inovação disruptiva para a conectividade, prometendo grandes mudanças na forma como trabalhamos e vivemos o próximo século. Nosso novo desafio é como vamos nos adaptar aos avanços apresentados por esta nova revolução (NGUYEN; DANG, 2018).

No horizonte das inovações tecnológicas, não restam dúvidas de que a tecnologia *Blockchain* como ferramenta para lidar com o *Big Data* é uma realidade cada vez mais presente no cenário mundial e nas mais diversas aplicações e diferentes áreas, sendo aclamada como a tecnologia mais disruptiva dos últimos anos. Seu uso na segurança pública não seria diferente, pois embora incipiente, é uma área onde cada vez mais surgem estudos e propostas da aplicabilidade desta ferramenta tecnológica.

2.3.6 Serviço público brasileiro *e blockchain*

No Brasil, existem diversos projetos em andamento focados no uso de *Blockchain* no setor público. Por exemplo, o BCPF e BCNPJ da Receita Federal são projetos criados com o objetivo de disponibilizar dados, via *Blockchain*, do Cadastro de Pessoas Físicas (CPF) e Jurídicas (CNPJ).[27] O TCU elaborou um guia sobre uso de *Blockchain*[28] no serviço público, no qual diversos exemplos em uso ou desenvolvimento são citados. O Sistema Alternativo de Liquidação de Transações (SALT) consiste em uma proposta de plataforma de contingência a ser utilizada em caso de pane do "Sistema de Transferência de Reservas". A Plataforma de Integração de Informações das Entidades Reguladoras (PIER) é a transparência e resposta célere às solicitações de IFs nos processos autorizativos, envolvendo o Bacen, a CVM e a Susep. E o Sistema Brasileiro de Poderes, que consiste em uma rede de *Blockchain* criada em parceria pelo BB e pela Petrobras, com o objetivo de digitalizar o processo de registro de poderes, que nada mais são do que permissões para movimentar as contas correntes de pessoas jurídicas (empresas ou governos estaduais/municipais) e vários outros casos.

A aplicabilidade pode ocorrer em diversas áreas, desde armazenamento de registros, atividades de negociação, gerenciamento da cadeia de suprimentos, sistema hipotecário, mercado imobiliário, distribuição de empregos, protegendo os direitos autorais, reivindicação de seguro, serviços de saúde, rede de internet das coisas. controle de licitações públicas governamentais, e certamente poderá utilizada na gestão da cadeia de custódia de evidências digitais.

2.3.6.1 Rede *Blockchain* Brasil

Em recente acordo de cooperação técnica, publicado no *Diário Oficial da União*, edição de 18 de abril, entre o Tribunal de Contas da União (TCU) e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) foi criada a Rede *Blockchain* Brasil[29]. Iniciou-se uma preparação para o uso futuro da tecnologia *Blockchain* em ações de controle externo, com o objetivo de trazer mais segurança para atos e contratos da administração pública, e a rede foi lançada em 30 de maio de 2022.

---

[27]https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2021/dezembro/entidades-publicas-terao-ate-31-12-para-adotar-novomecanismo-de-compartilhamento-de-dados-ou-pedir-prorrogacao

[28] https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm

[29] https://portal.tcu.gov.br/imprensa/noticias/tcu-e-bndes-lancam-rede-blockchain-brasil-nesta-segunda-feira.htm

A Rede *Blockchain* Brasil (RBB) é uma rede de instituições, de abrangência nacional, composta de estrutura de governança e infraestrutura tecnológica, que tem o objetivo de facilitar a adoção da tecnologia de *Blockchain* para a implementação de aplicações de interesse público. A criação da rede permitirá a otimização de recursos, redução de custos e remoção de barreiras de entrada para uso da tecnologia e a inovação no setor público. Seu código e descrição encontram-se disponíveis na plataforma *GitHub*.[30]

> A RBB foi fundada pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Tribunal de Contas da União (TCU), através de um Acordo de Cooperação, assinado em 12/04/2022. Instituições que desejarem participar da rede deverão submeter sua solicitação à Governança da RBB. a RBB a buscar o caminho de ser uma rede público-permissionada: "pública" porque poderá ser acessada por qualquer pessoa; "permissionada" porque os nós participantes do consenso precisam de permissão para participar. As redes público-permissionadas são uma solução adequada para aplicações de interesse público.
>
> *Blockchains* públicas são potencialmente muito interessantes para implantações focadas em transparência e confiança. Tal percepção é corroborada pelo Acórdão 1613/2020 do TCU que aponta como um dos seus maiores potenciais da tecnologia a implantação de medidas anticorrupção e pró-transparência. A possibilidade de implementar processos transparentes e que obedeçam ao princípio de compliance *by design* é uma grande oportunidade para organizações públicas. Porém, o uso de redes que melhor suportam estas características por instituições públicas apresenta barreiras de diversas naturezas, como por exemplo a aquisição de criptomoedas para remuneração do processamento na rede.
>
> Nas *blockchains* permissionadas, em geral privadas, os nós que realizam a validação das transações são conhecidos e previamente autorizados, de acordo com os requisitos e propósitos da rede, permitindo a determinação de responsabilidades e tratando a realização do processamento na rede como um compromisso de seus participantes. Porém, tais *blockchains* não permitem o acesso às informações pelo público em geral.
>
> Já nas *blockchains* público-permissionadas, é possível buscar um melhor modelo para aplicações de interesse público: a entrega de soluções de transparência e confiança através de redes públicas; e o menor custo e menor desafio tecnológico e regulatório das redes permissionadas. (ARANTES JUNIOR, 2021).

A Rede *Blockchain* Brasil (RBB) já funciona como uma base experimental para desenvolvedores que querem usar suas capacidades, garantindo o consenso entre as partes envolvidas por meio de *smart contracts*.

> O consenso na rede refere-se ao processo de obtenção de um acordo entre os participantes da rede quanto ao estado correto dos dados no sistema. O consenso leva a todos nós compartilhando exatamente os mesmos dados. Portanto, um algoritmo de consenso (i) garante que os dados no livro-razão sejam os o mesmo para todos os nós da rede e (ii) evita ataques maliciosos atores de manipular os dados. [...]
>
> Um *smart contract* é programa de computador que executa ações predefinidas quando certas condições dentro do sistema são atendidas. Os contratos inteligentes fornecem o idioma das transações, permitindo que o estado do livro-razão seja modificado. Eles podem facilitar a troca e transferência de qualquer ativo (por exemplo, ações, moeda, conteúdo, propriedade). eles residem na estrutura do *Blockchain* e são acionados junto com transações. Contratos inteligentes podem ser imaginados como protocolos

[30] https://github.com/RBBNet/rbb

> digitais usados para facilitar e reforçar a negociação de um contrato legal. Ações realizadas por pessoas de confiança terceiros durante uma negociação são substituídos por pedaços de código. (BELOTTI *et al*., 2019, tradução nossa)

Isso garante maior privacidade porque ninguém de fora pode ver o que está sendo enviado dentro de um ciclo de processamento de transações. As mais importantes características da RBB são sua escalabilidade (a rede pode processar até 24.000 transações por segundo) e a sua segurança (utiliza técnicas de criptografia para garantir que todos os dados são seguros e não podem ser adulterados). A implementação de *Blockchain* utilizada na RBB é a do projeto de código aberto *Hyperledger Besu,*[31] que é baseada na rede *Ethereum*.

Desta forma, pensar no uso de *Blockchain* para garantir a segurança e a imutabilidade dos registros e informações atrelados à cadeia de custódia das evidências criminais digitais seria uma evolução natural no processo criminal brasileiro e uma inovação no campo da Ciência Policial.

2.4 CONTRATOS INTELIGENTES

A grande maioria destes projetos descritos utilizam a *Blockchain* associada aos contratos inteligentes, que têm o potencial de revolucionar a maneira como a sociedade realiza negócios. Eles podem reduzir custos, aumentar a eficiência e melhorar a segurança. Além disso, eles também podem aumentar a transparência e a confiança entre as partes. Os *smart contracts* têm várias características que os tornam únicos, a saber:

- Autoexecutáveis: contratos inteligentes são autoexecutáveis, o que significa que eles podem iniciar uma ação ou transferir ativos automaticamente quando certas condições são cumpridas.
- Digitais: Além disso, eles são digitais, o que significa que podem ser armazenados e transferidos eletronicamente.
- Imutáveis: os *smart contracts* são imutáveis, o que significa que, uma vez criados, não podem ser alterados ou apagados.
- Descentralizados: os *smart contracts* são descentralizados, o que significa que não requerem intermediários, como advogados ou bancos.

[31] O *Hyperledger Besu* é um cliente *Ethereum* de código aberto desenvolvido sob a licença Apache 2.0 e escrito em Java. Funciona em redes públicas e privada, Fonte: https://besu.hyperledger.org/en/stable/

- Transparentes: Além disso, eles são transparentes, o que significa que todas as partes podem ver e verificar os termos do acordo.

Figura 8 - Funcionamento do contrato inteligente

Fonte: Adaptado e traduzido de https://101blockchains.com/pt/contratos-inteligentes-blockchain

Um contrato inteligente pode funcionar tanto como sendo único e junto com um grupo de contratos inteligentes. O único vai funcionar de forma independente. Os usuários podem definir um grupo de exemplos de contratos inteligentes entre si, já que precisam depender um do outro para concluir qualquer tarefa. O que precisa ser feito é definir as regras, termos e condições antes que qualquer contrato esteja pronto e colocar no contrato as informações que se deseja manter como registro; quando os requisitos são atendidos, o contrato é auto executado.

Todos os dados que entram na *Blockchain* através de um *smart contract* passam por uma função *hash* que utiliza a tecnologia de criptografia, garantindo a individualidade do conteúdo dentro dessa rede, como que gerando um selo de autenticidade digital. A tecnologia permite que qualquer pessoa possa consultar esse bloco e ver os dados que estão ali e todo histórico de transações daquele item, desde quem o criou, acessou ou detém a propriedade atual, atestando assim a individualidade e autenticidade.

3 PROCEDIMENTOS METODOLÓGICOS

Considerando a literatura dos trabalhos e a escassez de pesquisas sobre o tema, o presente estudo caracteriza-se como um estudo exploratório.

Na pesquisa exploratória, o objetivo é explorar uma área que pouco se conhece ou investigar as possibilidades de realizar determinado estudo (SWARAJ, 2019), como ocorre no presente trabalho. Não obstante, o estudo se caracteriza também como uma pesquisa descritiva, visto que possui o propósito de descrever um fenômeno (GIL, 1987): uso da tecnologia *Blockchain* e seus derivados como meio de preservar a cadeia de custódia de evidências digitais na investigação policial e o fluxo do processo da quebra de sigilo telemático.

A metodologia utilizada foi qualitativa. De acordo com Miles e Huberman, (1994), a pesquisa qualitativa fornece meios para desenvolver uma compreensão de fenômenos complexos a partir das perspectivas daqueles que estão vivendo. Os principais benefícios dos métodos qualitativos são que eles permitem ao pesquisador descobrir novas variáveis e relações, revelar e compreender processos complexos e ilustrar a influência do contexto social.

A seção apresenta o percurso metodológico para a realização da pesquisa e alcance dos objetivos previamente estabelecidos. O trabalho realizado foi organizado em algumas etapas descritas a seguir:

- Mapeamento bibliográfico e pesquisa sobre estudos aplicados ao arquivamento digital, armazenamento e custódia das evidências digitais apoiados na tecnologia *Blockchain* (tecnologia que possibilita manutenção da integridade, autenticidade e auditoria de seus dados);
- Esquematização do modelo do ciclo de vida das evidências digitais, dados oriundos de medidas cautelares de quebra de sigilo de dados telemáticos usados na investigação. Realizou-se uma representação gráfica do fluxo de trabalho e das atividades, com apoio do *software* Bizagi (modelagem do processo);
- Avaliação diagnóstica por meio questionário aplicado dentro da instituição Polícia Federal, no nicho de servidores que lidam com a temática de investigação com a quebra de sigilo telemático;
- E por fim, baseado na literatura, a sugestão de uma proposta de arquitetura de sistema apoiada pela tecnologia *Blockchain*, para gestão dos dados telemáticos na investigação criminal.

3.1 MAPEAMENTO DA LITERATURA

A fim de verificar os trabalhos existentes sobre o tema de interesse, realizou-se um mapeamento da literatura em março de 2022, tendo como base, principalmente, os questionamentos: como melhorar o processo de aquisição e o arquivamento digital das evidências digitais, dos dados obtidos pela quebra de sigilo telemático, envolvidos na investigação policial? Como eliminar o processo manual e individual do investigador (sua própria expertise) na gestão dos dados e da cadeia de custódia daquelas evidências digitais? Considerando a literatura dos trabalhos e a variedade de pesquisas sobre o tema, o presente estudo caracteriza-se como sendo um estudo exploratório.

Para tanto, foram selecionadas as bases de dados que se mais se relacionavam com o assunto. Foram consultados e selecionados trabalhos através das bases de publicações científicas ScienceDirect, Web of Science, Scopus e IEEE Xplore. A seleção das bases se sustentou na relevância de cada uma delas no meio acadêmico e científico e na área de domínio de suas coleções.

3.1.1 Busca e seleção dos estudos

Inicialmente, foram escolhidos termos relacionados à tecnologia *Blockchain* e armazenamento e o envolvimento na investigação policial. Foram pesquisados os termos combinados nos títulos dos artigos: "*digital forensics*", "*digital evidence*", "*Blockchain"*, "*chain of custody*", "*law enforcement*". O período escolhido para a pesquisa foi a partir do ano de 2012, apesar de a primeira publicação a respeito do uso de *Blockchain* ser anterior (NAKAMOTO, 2009), pois entendemos que o uso do protocolo se difundiu e amadureceu a partir do ano de 2012. Nas tabelas abaixo, resumiu-se o trabalho realizado. Somente artigos e trabalhos de conferência foram pesquisados demais publicações como livros foram excluídos.

Tabela 1 - *Strings* de pesquisas utilizadas

BASE DE DADOS	CAMPO	STRING DE PESQUISA - INGLÊS	QTDE
Web of Science	Title	(TI=(Digital Forensics or Digital Evidence)) AND TI=(*Blockchain*)	24
		((TI=(Digital Evidence)) AND TI=(Blockchain)) AND TI=(law enforcement)	0
		(TI=(chain of custody)) AND TI=(Blockchain)	10
Scopus	Title	**STRING DE PESQUISA - INGLÊS**	**QTDE**

		(TITLE ("digital forensics") OR TITLE ("digital evidence") AND TITLE (blockchain))	30
		(TITLE ("law enforcement") AND TITLE ("digital evidence") AND TITLE (blockchain))	0
		(TITLE ("chain of custody") AND TITLE (blockchain))	14
IEEE Xplore	Title	**STRING DE PESQUISA - INGLÊS**	**QTDE**
		((("Document Title": "Digital Evidence" OR "Document Title": "Digital Forensics") AND ("Document Title": Blockchain)))	16
		(("Document Title": "law enforcement" AND "Document Title":"Digital evidence") AND "Document Title": blockchain)	0
		("Document Title":chain) AND ("Document Title":custody) AND ("Document Title":blockchain)	4
ScienceDirect	Title	**STRING DE PESQUISA - INGLÊS**	**QTDE**
		Title: ("Digital Evidence" OR "Digital Forensics") AND Blockchain	45
		Title: ("law enforcement") AND "digital evidence" AND blockchain	11
		Title: "chain of custody" AND Blockchain	23
TOTAL			**177**

Fonte: O autor (2022).

3.1.2 Extração dos dados e resultados

Na primeira etapa da pesquisa, das 177 publicações, 36 foram excluídas por serem repetidas; 124 foram excluídas por não estarem no contexto da pesquisa ou não serem do interesse do trabalho; 5 foram excluídas por estarem com acesso pago/fechado; e as demais foram selecionadas.

Ao final, doze publicações foram selecionadas como relevantes para o presente estudo, conforme a Tabela 3:

Tabela 2 - Resultados dos principais artigos selecionados

	TÍTULO DO TRABALHO	AUTORES	ANO
1	Storing and Securing the Digital Evidence in the Process of Digital Forensics through *Blockchain* Technology	Anne et al	2021
2	LEChain: A *Blockchain* -based lawful evidence management scheme for digital forensics	Li, M. et al	2021
3	Distilling blockchain requirements for digital investigation platforms	Olukoya, O.	2021
4	MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture	Khan, A. et al	2021
5	B-CoC: A *Blockchain* -Based Chain of Custody for Evidence Management in Digital Forensics	Bonomi, S. et al	2020
6	Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain	Petroni, C. A. et al	2020
7	Blockchain-based Chain of Custody - Towards Real-time Tamper-proof Evidence Management	Ahmad, L. et al	2020

8	Block-DEF: A secure digital evidence framework using *Blockchain*	Tian, Z. H. et al	2019
9	Digital Forensics: Maintaining Chain of Custody Using *Blockchain*	Chopade, M. et al	2019
10	Digital forensics using *Blockchain*	Gopalan, S. H. et al	2019
11	Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer	Lone, A.H et Al	2019
12	Chronological independently verifiable electronic chain of custody ledger using blockchain technology	Burri, X. et al.	2019

Fonte: O autor (2022)

Além destes resultados, a leitura dos artigos pesquisados apontou referências bibliográficas de interesse em seu corpo, algumas citadas no texto do trabalho e referenciadas adequadamente.

Da análise da literatura dedicada ao tema, percebeu-se que a investigação policial ainda carece de um suporte mais robusto para tratar os dados telemáticos envolvidos diretamente na investigação policial.

3.2 PESQUISA INTERNA – AVALIAÇÃO DIAGNÓSTICA

A etapa de Diagnóstico foi realizada através de uma avaliação diagnóstica por meio de questionário aplicado dentro da Instituição Polícia Federal, no nicho de servidores que lidam com a temática de investigação com o uso de evidências digitais (quebra de sigilo telemático).

Os convidados responderam a um questionário objetivo, com seis perguntas e com 3 a 5 opções de respostas, sendo cerca de 50 servidores que tiveram ou têm atuação com o manuseio de dados telemáticos. As questões foram elaboradas e respondidas por meio da plataforma Google, na ferramenta *Google Forms*. Esta avaliação preliminar não esgota o assunto e muito menos elimina um diagnóstico mais profundo e preciso; no entanto, as respostas foram bastante esclarecedoras, corroborando o direcionamento desta pesquisa.

3.2.1 Universo

Foi realizada uma avaliação diagnóstica por meio de questionário aplicado dentro da instituição Polícia Federal, no nicho de servidores que lidam com a temática de investigação com o uso de evidências digitais (quebra de sigilo telemático).

Os convidados, cerca de 50 servidores que tiveram ou têm atuação com o manuseio de dados telemáticos, responderam a um questionário objetivo, com seis perguntas, cada qual com 3 a 5 opções de respostas.

3.2.2 Coleta de dados

Os dados foram coletados a partir de um questionário objetivo divulgado no ambiente interno da Polícia Federal (grupo corporativo de mensagens instantâneas), contendo seis perguntas com 3 a 5 opções de respostas. No grupo com cerca de 100 servidores voltados a análise e inteligência policial, responderam apenas cerca de 50 servidores que tiveram ou têm atuação com o manuseio de dados telemáticos. O método utilizado foi a elaboração de perguntas e respostas por meio da plataforma Google, pela ferramenta *Google Forms*.

3.2.3 Tratamento e análise dos dados

Salientamos que, dentre as opções de respostas em algumas questões, havia a opção "outros", que foi respondida de forma descritiva pelos servidores e continha elementos de confidencialidade, representando um pequeno percentual nos gráficos apresentados. Por esse motivo, tiveram suas legendas ocultas por conterem informações sensíveis e pela manutenção da segurança da informação.

Os resultados que tiveram suas legendas ocultas ocorreram nos pequenos percentuais representados nos gráficos e não afetaram as respostas majoritárias.

3.3 MODELAGEM DO PROCESSO

A modelagem de processos de negócios é um mecanismo de representação gráfica que ajuda a melhorar a compreensão de um contexto, as etapas realizadas, as validações e regras de negócios que fazem parte de seu universo (PASTRANA-PARDO et al., 2022).

Foi elaborada uma representação gráfica com o fito de esquematizar o modelo do ciclo de vida dos dados oriundos de medidas cautelares de quebra de sigilo de dados telemáticos usados na investigação. Desta forma, foi feita uma modelagem do processo, uma representação gráfica do fluxo de trabalho e das atividades, com apoio do software Bizagi.

4 TRABALHOS RELACIONADOS

Depois do mapeamento da literatura relacionada, identificamos diversas propostas com características diferentes de utilização da tecnologia Blockchain para apoio à cadeia de custódia de evidências digitais. Todas visando fornecer integridade, preservação, transparência e resistência à adulteração das evidências, em todo o ciclo de vida, da coleta de evidências até a preservação e no manuseio por várias partes interessadas ao mesmo tempo. Nenhum dos trabalhos abordou a aquisição de evidências digitais por meio das plataformas de requisições de autoridades da lei das empresas de tecnologia. Assim, sugerimos um modelo de arquitetura para atender esta característica.

4.1 ARTIGO 1 – ARMAZENANDO EVIDÊNCIAS DIGITAIS COM *BLOCKCHAIN*

Anne *et al.* (2021) ressaltam a importância que a evidência tem no caso investigado, desempenhando papel vital no julgamento. Se tal evidência for adulterada, a verdade será alterada e a justiça não poderá prevalecer em tal situação. Propõem, então, a utilização da tecnologia *Blockchain,* que possui propriedades de alta segurança. Na tecnologia *Blockchain,* um registro na rede possui um *hash* com o registro anterior, gerando um encadeamento criptografado, o que garante a imutabilidade no livro-razão e, assim, nas evidências digitais. Portanto, se um registro precisa ser alterado, o registro anterior precisa ser alterado, o que é difícil quando há milhares de registros na cadeia. Assim, o problema da manipulação de evidências é resolvido pelas propriedades da tecnologia *Blockchain.*

4.2 ARTIGO 2 – LECHAIN

Li *et al.* (2021) sugerem uma arquitetura chamada de LEChain, um esquema de gerenciamento de evidências legais baseado em *Blockchain* para supervisionar todo o fluxo de

evidências e todos os dados do Judiciário (por exemplo, votos e resultados de julgamentos), estendendo-se desde a coleta de provas e acesso durante a investigação policial até a votação do júri nos julgamentos. Especificamente, utiliza assinaturas aleatórias curtas para autenticar anonimamente as identidades das testemunhas e proteger sua privacidade. Uma *Blockchain* de consórcio registra as transações de evidências e implementa um protótipo baseado em uma rede local de teste *Ethereum*. No LEChain, a TA (autoridade confiável) é uma agência governamental e inicializa todo o sistema; o Departamento de Polícia, o Tribunal e a Prisão são os quatro mineradores de *Blockchain*. Os mineradores mantêm a *Blockchain* validando transações de *upload*/acesso e executando o *Proof-Of-Authority* (PoA) como seu mecanismo de consenso.

4.3 ARTIGO 3 – THEHIVE BLOCKCHAIN NA INVESTIGAÇÃO DIGITAL

Olukoya, O. (2021) descreve que, ao lidar com incidentes de segurança da informação, existem muitas informações que precisam ser armazenadas, processadas e analisadas e o gerenciamento de casos de incidentes de segurança permite que um analista de segurança adicione logs relacionados. O autor reconhece que na literatura existem trabalhos que têm como foco manter a integridade da evidência, o livro-razão de uma *Blockchain* se mostra inviolável para plataformas de resposta a incidentes de segurança.

O foco do trabalho de pesquisa é propor metodologias e frameworks para a aplicação de *Blockchain* para auxiliar investigações de segurança cibernética. O serviço *Blockchain* é executado em infraestruturas críticas como uma medida de serviço proativo para registrar ações na resposta e investigação de incidentes. A estrutura proposta serve para garantir a integridade de ações investigativas forenses digitais e os dados de evidências. Tendo como objetivo registrar todas as atividades de execução e qualquer ação no caso gerenciado na plataforma de resposta a incidentes, de uma maneira cronológica e funcionado como um sistema eletrônico verificável independente. No entanto, por serem as investigações digitais muito sensíveis, exigindo confidencialidade e segurança dos usuários envolvidos, a solução proposta no trabalho é uma blockchain privada, e com consenso autorizado e ainda suportar contratos inteligentes. Para tal o autor escolheu a infraestrutura *Blockchain* da *HyperLedger Fabric*[32], que é uma

[32] O Hyperledger Fabric, um projeto de código aberto da Linux Foundation, é a estrutura blockchain modular e padrão de fato para plataformas blockchain corporativas. Fonte: https://www.hyperledger.org/

infraestrutura com blockchain permissionada, escolhida porque é uma rede privada, com usuários autorizados e permitindo uma lógica de contrato inteligente.

4.4 ARTIGO 4 – MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture

Neste trabalho, Khan, A. *et al* (2021), pretendem um processo de investigação forense digital seguro e transparente usando a tecnologia blockchain. A chamada MF-Ledger é uma proposta, baseada na *Blockchain hyperledger,* de arquitetura de investigação forense digital nova, segura e eficiente, onde as partes interessadas participantes criam uma rede privada para troca e consenso das diferentes atividades de investigação antes de estas serem armazenadas no livro-razão da *Blockchain,* por meio de uso de contratos inteligentes. Uma infraestrutura com *Blockchain* permissionada, em uma rede privada, A solução proposta oferece integridade de informações, prevenção e mecanismo de preservação robustos para armazenar de forma permanente e imutável as evidências (cadeia de custódia) em um livro-razão criptografado com permissão.

4.5 ARTIGO 5 – B-COC

Bonomi *et al*. (2018) propuseram uma cadeia de custódia baseada em *Blockchain* (B-CoC) para desmaterializar o processo da cadeia de custódia manual, garantindo a integridade auditável das evidências coletadas e a rastreabilidade dos proprietários. Desenvolveram um protótipo de B-CoC baseado em *Ethereum* e avaliaram o seu desempenho. A arquitetura de cadeia de custódia baseada em *Blockchain* (B-CoC) proposta neste trabalho foi baseada em uma *Blockchain* privada e permissionada. Esta escolha foi motivada pela autenticação requisito do processo de cadeia de custódia (CoC), que não permite que partes não autorizadas e não confiáveis gerenciem evidências digitais e, portanto, estejam na rede.

4.6 ARTIGO 6 – CONTRATOS INTELIGENTES NA CADEIA DE CUSTÓDIA DIGITAL

Conforme aponta Petroni, C. et al (2020) em seu trabalho, o setor público tem agido um pouco tarde na construção de competências, inclusive as de natureza jurídica, e apenas observando as oportunidades de aperfeiçoamento de seus procedimentos operacionais, principalmente no que diz respeito à legislação específica para a busca, armazenamento e manutenção de evidências digitais. Estas permanecem numa cadeia digital de custódia de responsabilidade do próprio tribunal e organizado de acordo com os artefatos que possui ou a competência específica de um perito nomeado pelo tribunal. A avaliação desse tipo de prova requer expertise pouco conhecida pelos juízes. Além disso, evidências digitais típicas podem ser acessadas por socorristas, delegacias de polícia, investigadores, peritos, promotores, advogados de defesa e podem até ser corrompidas por pessoas anônimas com acesso oculto às evidências.

Para solucionar o cenário descrito, propõe um sistema direcionado aos participantes envolvidos na cadeia de custódia das evidências legais digitais baseadas em *Blockchain* para garantir os requisitos legais. Desta forma, a plataforma proposta permite, além do necessário armazenamento de provas digitais, a consulta por operadores do direito, os responsáveis pela execução processo, como advogados, juízes e promotores. Auxiliando no armazenamento das evidências digitais coletadas por especialistas e na adoção de mecanismos padronizados que permitem que outros operadores de aplicação da lei acessem, mantenham e usem a cadeia de custódia de evidências digitais na forma da lei, dentro da total garantia de integridade e confiabilidade. A plataforma se utiliza de contratos inteligentes aplicados numa rede *Blockchain* pública e permissionada na plataforma *Ethereum*.

4.7 ARTIGO 7 –GERENCIAMENTO DE EVIDÊNCIAS À PROVA DE VIOLAÇÃO

Neste artigo, Ahmad, L. *et al* (2020), propõe uma cadeia de custódia segura por meio de um *framework*, utilizando a tecnologia blockchain para armazenar os metadados da evidência enquanto a evidência é armazenada em um meio de armazenamento. A estrutura é construída em cima de uma derivação da rede *Ethereum*, no serviço de nuvem do google, oferecendo uma *Blockchain* híbrida, permitindo que a organização autorizada detenha o controle sobre os dados, reduzindo gastos com a criação de uma rede própria e ainda usufruindo de uma rede com grande velocidade das transações. Atendendo a demanda para documentar cada transmissão do momento em que as provas são apreendidas, garantindo assim que as provas possam ser acessadas ou possuídas apenas por pessoas autorizadas.

O *framework* é integrado com o sistema de evidência digital onde as evidências são armazenadas fisicamente e bloqueadas usando códigos inteligentes. Para garantir a sequência de envio e recuperação de evidências, apenas uma parte autorizada pode possuir o código que poderá desbloquear a evidência. A estrutura proposta oferece uma solução segura que mantém integridade da evidência e admissibilidade entre várias partes interessadas como agências de aplicação da lei, advogados e peritos profissionais.

4.8 ARTIGO 8 – BLOCK-DEF

Tian *et al.* (2019) propuseram uma estrutura de evidência digital chamada Block-DEF, que é baseada em *Blockchain* para apoiar a coleta, armazenamento, verificação e recuperação de evidências. Seu *design* armazena as informações de evidências na *Blockchain* e preserva as evidências em uma plataforma de armazenamento confiável. Eles usaram dois esquemas de assinatura múltipla para envio e recuperação de evidências, de modo a garantir a rastreabilidade. No entanto, sua fase de acesso à evidência não considera os atributos dos solicitantes de evidência. Os resultados analíticos e experimentais mostrados no trabalho apontam que o Block-DEF é uma estrutura escalável, garante a integridade e validade das evidências e equilibra bem a privacidade e a rastreabilidade.

4.9 ARTIGO 9 – CADEIA DE CUSTÓDIA BASEADA EM *BLOCKCHAIN* COM *HYPERLEDGER*

Chopade *et al*. (2019) citam como principal problema da cadeia de custódia a documentação e registro da interação com a evidência, além de seu uso por várias partes, associando um risco de adulteração. Propõem, então, um sistema baseado em *Blockchain* usando *Hyperledger*, no qual as evidências estão sendo transferidas, registradas e atualizadas com segurança. As transações podem ser rastreadas, pois todas são armazenadas no *Blockchain* com segurança, utilizando um algoritmo de criptografia Base64 para criar *hash* da imagem da evidência. A evidência em si não é passada com os dados na cadeia, somente o valor de *hash*. Os dados textuais codificados garantem fácil transporte pelas redes sem chances de perda de dados.

4.10 ARTIGO 10 – FORENSE DIGITAL USANDO *BLOCKCHAIN*

Gopalan (2019) enfatiza premissas básicas ao considerar a integridade da evidência eletrônica. E propõe o uso de *Blockchain* para garantir a integridade do sistema e preservar a integridade das evidências para que possam ser aceitas judicialmente. Considera que a cadeia de custódia (CoC) possui etapas necessárias que um investigador criminal deve seguir para garantir que as informações sejam honestas. Os principais requisitos de um processo de CoC são: a integridade e a rastreabilidade. Aproveitando esses recursos, o autor definiu uma arquitetura capaz de suportar o processo de CoC criando uma *Blockchain* pública e permissionada para impor um contrato inteligente que acompanhe as mudanças de posse ao longo do ciclo de vida da prova.

Diante da pesquisa entre os trabalhos relacionados, resumimos na Tabela 4, a seguir, apontamos a tecnologia comum indicada pelos autores.

4.11 ARTIGO 11 – CADEIA DE NO HYPERLEDGER COMPOSER

Lone, A. *et al* (2019), descreve a extrema importância garantir a integridade, autenticidade e auditabilidade da evidência digital conforme ela se move ao longo de diferentes níveis de hierarquia na cadeia de custódia durante a investigação de crimes cibernéticos. E ressalta que, elas desempenham um papel importante na investigação de crimes cibernéticos, pois são usadas para vincular indivíduos a atividades criminosas. Desta forma, propõe uma cadeia de custódia forense digital baseada em *Blockchain*, trazendo integridade e resistência à adulteração para a cadeia de custódia forense digital.

O modelo proposto foi construído no *Hyperledger Composer*[33], uma Blockchain permissionada de consórcio ou privada (onde uma única organização controla). Assim, as informações sobre a evidência são confinadas apenas aos participantes que fazem parte do *Blockchain*, autorizado por administradores pertencentes a organização do consórcio. Os participantes podem compartilhar informações de forma confidencial com a ajuda de canais na

[33] *Hyperledger* Composer é uma versão anterior ao *Hyperledger Fabric,* ambos da de código aberto da Linux Foundation.

estrutura do *Hyperledger*. A opção foi escolhida por ser mais adequada para simular as funções do sistema de justiça criminal atual na prática, devido à sua natureza pública e ao mesmo tempo permissionada, inerente a heterogeneidade e complexidade do atual sistema judiciário.

4.12 ARTIGO 12 – LIVRO-RAZÃO ELETRÔNICO DE CADEIA DE CUSTÓDIA

Burri, X. *et al.* (2019) descreve de forma clara o problema da cadeia de custódia de evidências digitais, onde há uma necessidade premente para uma maneira confiável e transparente de manter a cadeia de custódia eletrônica (e-CoC) e a integridade das informações. Geralmente, um valor *hash* de evidência digital é calculado e documentado com os dados adquiridos para provar que não foi alterado. No entanto, o valor de *hash* sozinho não prova que a evidência digital é a mesma de quando foi obtida, apenas que o conteúdo não foi modificado desde o momento em que o *hash* foi calculado.

O trabalho respondeu a esta necessidade com um livro-razão (*ledger*), cronológico, independente e verificável usando a tecnologia *Blockchain*. Empregando essa abordagem, cada registro é armazenado em um bloco, sendo cada bloco conectado ao anterior com o valor de *hash* do bloco. Esta *Blockchain* pode ser hospedada por uma entidade confiável e acessada por qualquer parte para verificar os detalhes da cadeia de custódia. Por motivos de privacidade, as informações confidenciais não são armazenadas nos registros da *Blockchain*. Além disso, para provar que o próprio *ledger* não foi modificado, as informações são enviadas periodicamente para um *Blockchain* público, onde a integridade é garantida por sua descentralização e pela estrutura de um ledger seguro. Nem todos os blocos são enviados para uma *Blockchain* pública que permite diferentes níveis de verificação. Demonstrando que este *ledger* pode ser usado por diferentes partes em um contexto legal, incluindo profissionais forenses digitais, advogados e juízes.

4.13 *BLOCKCHAINS* NOS TRABALHOS RELACIONADOS

Na tabela abaixo, resumimos os trabalhos mais relevantes encontrados no mapeamento da literatura.

Tabela 3 - Tipos de *Blockchains* nos trabalhos relacionados

TRABALHO	AUTORES	TIPO DE BLOCKCHAIN
B-COC: a blockchain -based chain of custody for evidence management in digital forensics	Bonomi, S. et al	**Privada**
Blockchain-based chain of custody - towards real-time tamper-proof evidence management	Ahmad, L. et al	**Híbrida**
BLOCK-DEF: a secure digital evidence framework using blockchain	Tian, Z. H. et al	**Consórcio ou Privada**
Chronological independently verifiable electronic chain of custody ledger using blockchain technology	Burri, X. et al.	**Híbrida**
Digital forensics using blockchain	Gopalan, S. H. et al	**Consórcio**
Digital forensics: maintaining chain of custody using blockchain	Chopade, M. et al	**Consórcio**
Distilling blockchain requirements for digital investigation platforms	Olukoya, O.	**Privada**
FORENSIC-CHAIN: blockchain based digital forensics chain of custody with poc in hyperledger composer	Lone, A.H et Al	**Consórcio ou Privada**
LECHAIN: a blockchain -based lawful evidence management scheme for digital forensics	Li, M. et al	**Consórcio**
Mf-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture	Khan, A. et al	**Privada**
Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain	Petroni, C. A. et al	**Híbrida**
Storing and securing the digital evidence in the process of digital forensics through blockchain technology	Anne et al	**Privada**

Fonte: Elaborado pelo autor (2023).

Como pode ser observado, a maioria dos pesquisadores apontaram em seus trabalhos a utilização das redes de consórcio ou privada como sendo a solução adequada em seus casos.

5 GESTÃO DOS DADOS TELEMÁTICOS E O SEU CICLO DE VIDA

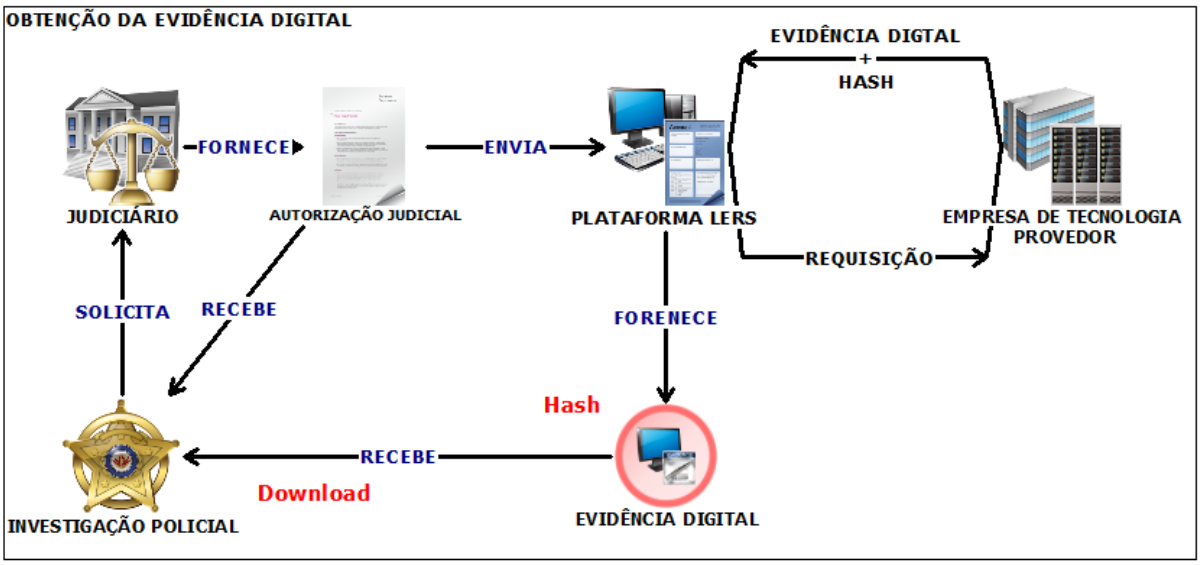
Segundo Borri (2019), o processo penal brasileiro, que prima pela busca da verdade, evidencia-se, em regra, pela liberdade probatória. Assim, qualquer meio de prova é admitido,

desde que não viole a lei, a moral e os bons costumes. Veda-se a prova ilícita, incluindo as que violam regras de ordem processual (provas ilegítimas) e de direito material (provas ilegais). Logo, para o ordenamento jurídico brasileiro, em especial no que tange à prova digital, objeto da presente discussão, a observância do princípio da vedação da prova ilícita é corolário do devido processo legal. Desta forma, a obtenção das provas digitais junto às empresas de tecnologia será realizada mediante a devida ordem judicial e respeitando-se todos os princípios legais. Deverá, ainda, ser respeitada a cadeia de custódia em todo o seu ciclo de vida, desde a aquisição ao descarte dos dados.

5.1 AQUISIÇÃO DOS DADOS

Na investigação durante a realização de diligências extraordinárias, como a representada pela medida cautelar de quebra de sigilo telemático, após fundamentação dos pedidos e representação da autoridade policial e deferimento pela justiça, o investigador tem o instrumento necessário, uma ordem judicial, para solicitar junto aos provedores e empresas de tecnologia os dados convenientes ao processo investigativo, conforme autorizado explicitamente.

Figura 9 - Ciclo de obtenção de evidência digital



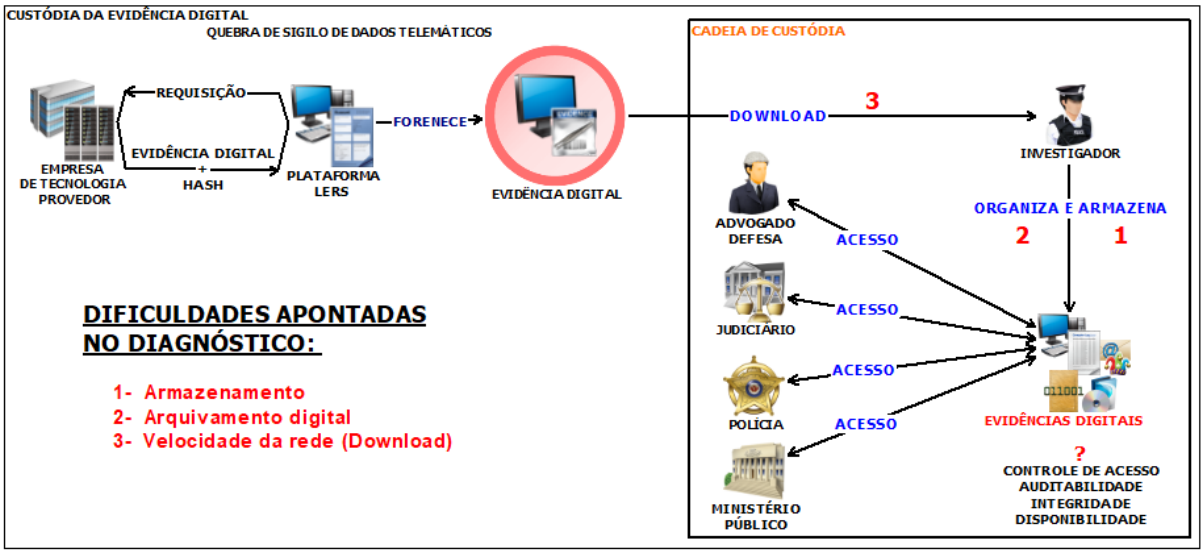
Fonte: O autor (2022)

Nesta etapa aquisição dos dados, o investigador precisa interagir com a plataforma de requisições das empresas de tecnologia para o envio da ordem judicial, através de seus portais de atendimentos a autoridades e logo após o processamento o investigador realiza o *download* dos dados diretamente na mesma plataforma onde se encontram os dados solicitados, extraídos de forma forense com os *hashes* dos arquivos (Figura 9).

5.2 MANUSEIO DOS DADOS

A partir deste momento, com a realização deste *download* de arquivos inicia-se a etapa de manuseio dos dados, onde a cadeia de custódia da evidência digital conta com a participação direta do investigador, processo fragilizado pela interação humana. E conforme identificado na pesquisa diagnóstica, as maiores dificuldades seriam armazenamento, organização (arquivamento digital) e velocidade da rede (Figura 10).

Figura 10 - Ciclo de vida da evidência digital fragilizado



Fonte: O autor (2022)

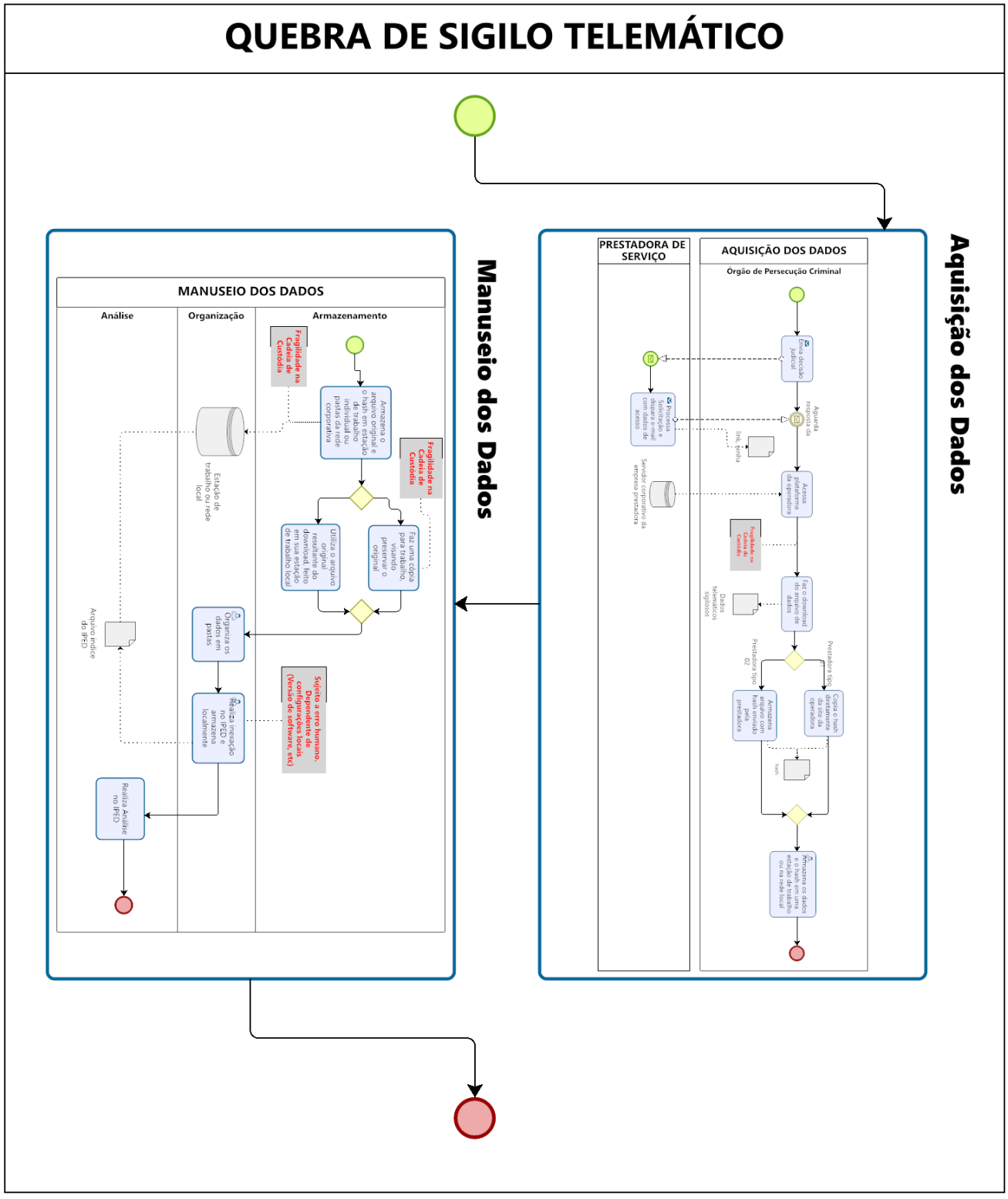
Neste ambiente, o investigador e sua cognição, a interação humana, respondem diretamente pelo ciclo de vida da evidência e sua cadeia de custódia. Têm o controle e a personalização da coleta, arquivamento digital preliminar e armazenamento dos dados fornecidos, abrindo possibilidade de falhas ou comprometimento da prova criminal nos trabalhos investigativos. Além de controle precário das interações e manuseio das evidências na cadeia de custódia.

5.3 MODELAGEM DO PROCESSO – CICLO DE VIDA DOS DADOS

A modelagem do processo foi realizada por meio de uma representação gráfica do fluxo de trabalho e das atividades, com apoio do *software* Bizagi. Utilizou-se o *Business Process Model and Notation* – BPMN, notação da metodologia de gerenciamento de processos de negócio que trata de uma série de ícones padrões para o desenho de processos, o que facilita o entendimento do usuário e a representação gráfica do fluxo de trabalho e das atividades.

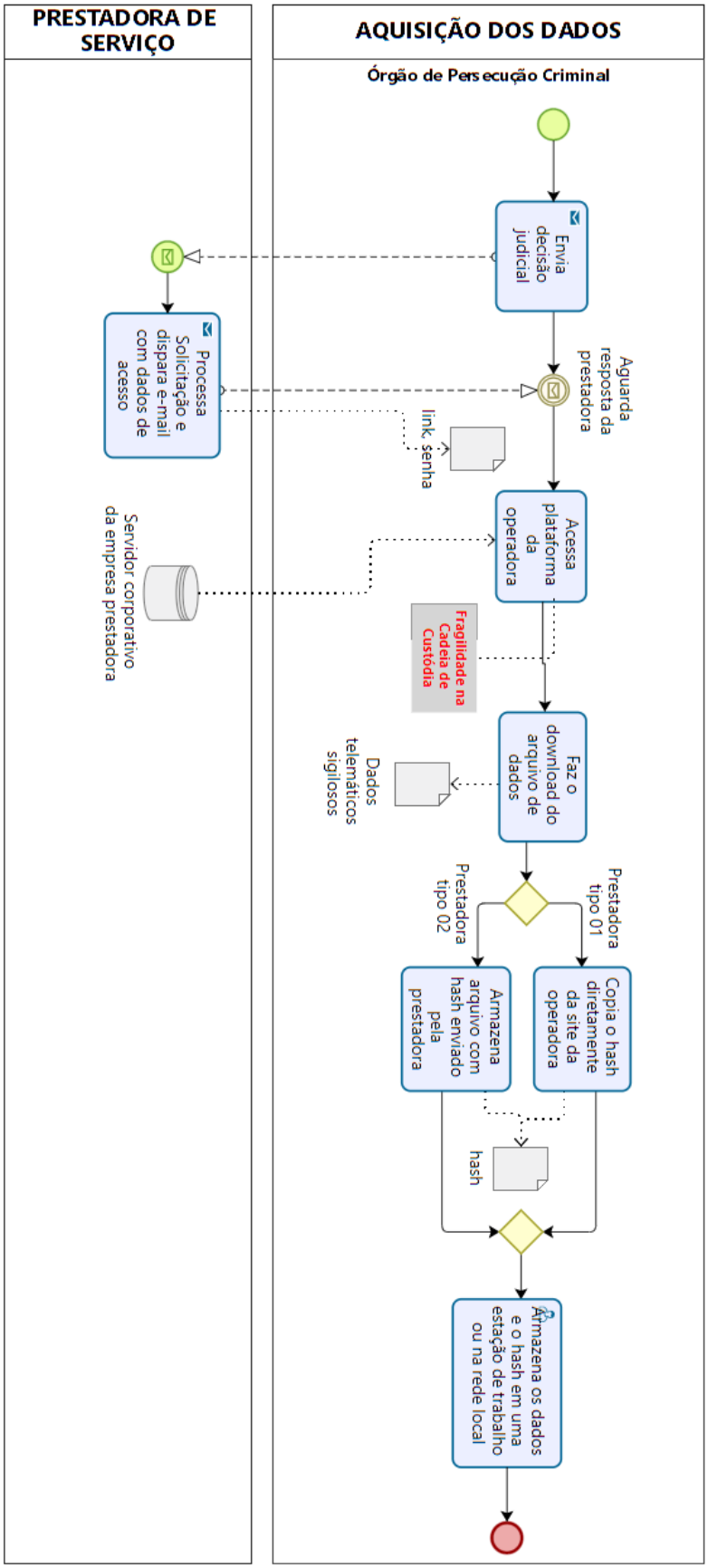
Os fluxos gerais dos processos de aquisição e manuseio dos dados são apresentados na figura abaixo (Figura 11) e nas seguintes (Figura 12 e 13), nas quais são detalhadas as duas etapas separadamente.

Figura 11 – Modelagem quebra de sigilo – Geral



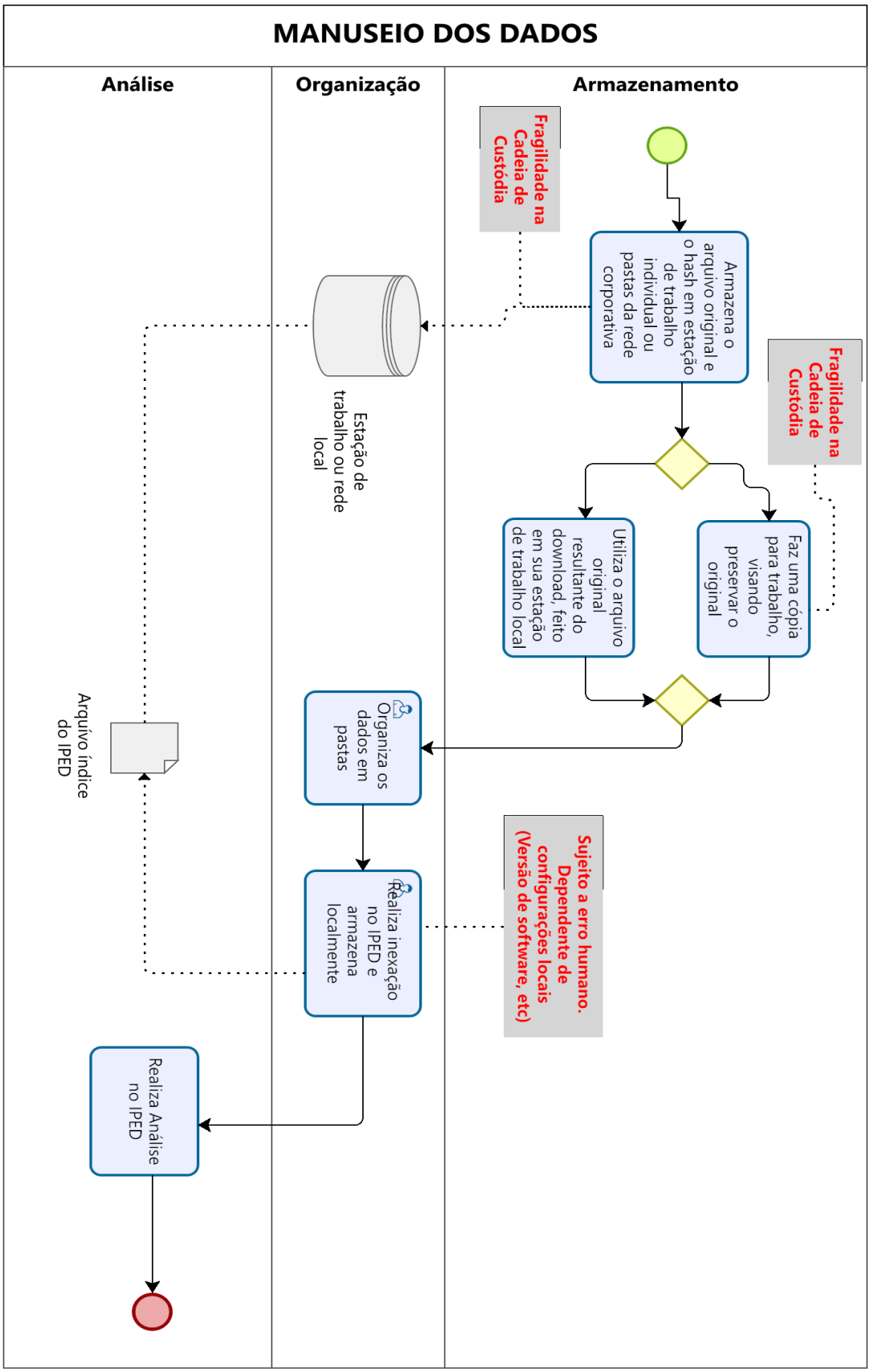
Fonte: O autor (2022)

Figura 12 – Modelagem – Aquisição de dados



Fonte: O autor (2022)

Figura 13 – Modelagem – Manipulação dos dados



Fonte: O autor (2022)

6 RESULTADOS DO DIAGNÓSTICO

Os resultados obtidos com a pesquisa reafirmaram a existência de problemas na gestão dos dados telemáticos e os efeitos danosos que podem trazer ao processo da persecução criminal. Esses problemas são particularmente críticos nas áreas de armazenamento, organização (arquivamento digital) e velocidade da rede, conforme identificado no diagnóstico.

O quadro a seguir resume as principais falhas identificadas nesses três pontos cruciais da cadeia de custódia dos dados telemáticos. Para cada uma dessas falhas, a solução proposta oferece melhorias significativas, integrando tecnologias como Blockchain para garantir a segurança, a padronização e a eficiência dos processos de gestão de evidências digitais.

Quadro 2 – Falhas e Soluções e Modelos

Falha na Cadeia de Custódia Atual	Componentes da Solução Proposta	Comparação com Outros Modelos
Armazenamento Disperso e Inseguro	Solução que integra segurança no armazenamento com monitoramento contínuo e registro de todas as interações	**MF-Ledger (Khan et al., 2021):** Adota medidas de segurança e integridade, mas com maior complexidade de implementação.
Falta de Padronização na Organização e Arquivamento Digital	Plataforma Web baseada em Blockchain, que padroniza e automatiza o fluxo de trabalho	**LEChain (Li et al., 2021):** Oferece padronização, mas com foco em uma rede privada específica.
Baixa Velocidade e Eficiência na Transmissão de Dados	Blockchain que otimiza o processo de transmissão e rastreamento de dados em tempo real	**TheHive (Olukoya, 2021):** Inclui funcionalidades de auditoria, mas com foco específico em segurança cibernética.
Risco de Manipulação de Evidências	Blockchain que garante a imutabilidade e integridade dos dados em todas as etapas do processo	**B-CoC (Bonomi et al., 2018):** Utiliza Blockchain para rastreabilidade, mas com menos flexibilidade na integração.
Dependência de Interação Humana e Risco de Erro	Automação dos processos críticos de aquisição, armazenamento e arquivamento digital	**Smart Contracts na Cadeia de Custódia (Petroni et al., 2020):** Usa contratos inteligentes, mas com foco restrito a certas jurisdições.

Fonte: O autor (2022)

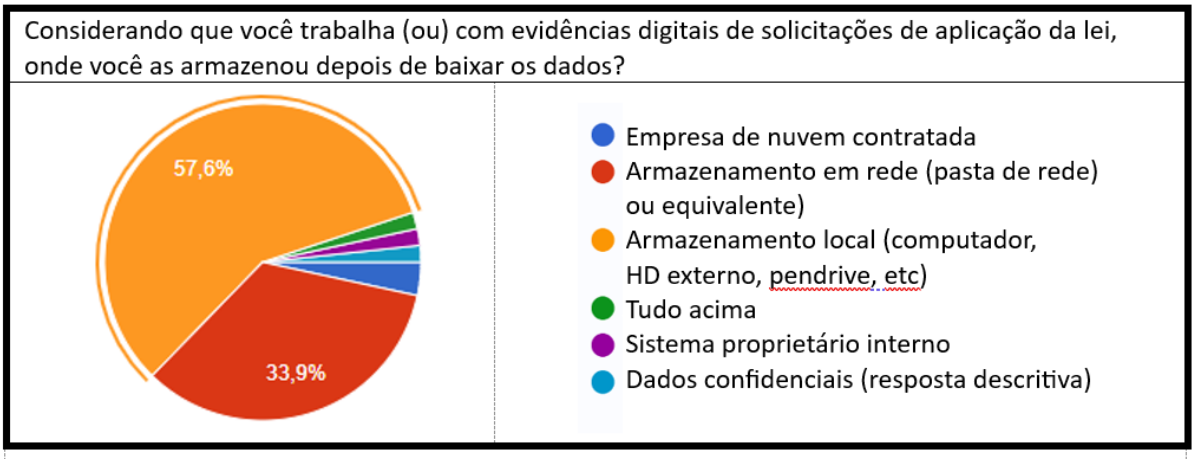
Nos capítulos seguintes, apresentaremos e analisaremos os resultados dos questionários aplicados, detalhando as percepções sobre os desafios em armazenamento, organização (arquivamento digital) e velocidade da rede. Através dos gráficos gerados, exploraremos como esses pontos críticos foram identificados e seus impactos no processo de gestão das evidências digitais.

6.1.1 Infraestrutura de armazenamento

Ao realizar o *download* dos dados da empresa de tecnologia (após todo o rito legal e apropriado), o investigador precisa de espaço para armazenamento e dispositivos de armazenamento adequados. As evidências digitais precisam ser mantidas o tempo necessário do processo criminal e pode levar até 3 anos dependendo do caso.

A pesquisa diagnóstica preliminar apontou para um percentual de 58% de um armazenamento local (computador ou estação de trabalho, HDs externos ou *pendrives*) e de 34% utilizaram a infraestrutura de armazenamento em rede (pastas de rede) existentes na instituição (Figura 14).

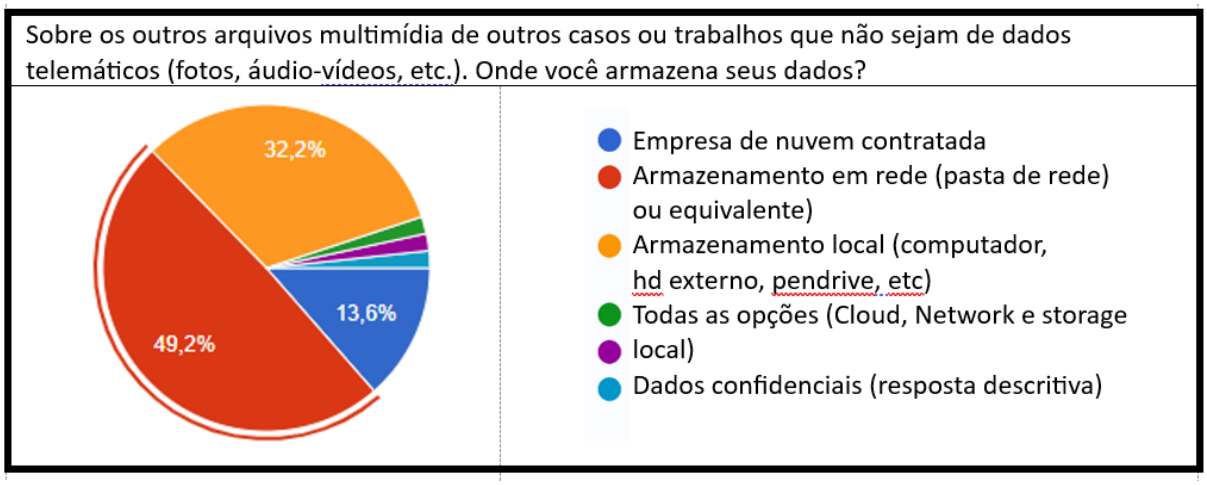
Figura 14 - Principal armazenamento - dispositivos locais



Fonte: O autor (2022).

Em relação a outros arquivos e evidencias de casos e trabalhos realizados que não são relacionados com requisições de dados telemáticos, o armazenamento preferido é o armazenamento em rede com 49% das respostas, seguido pelo armazenamento local com 32% (Figura 15).

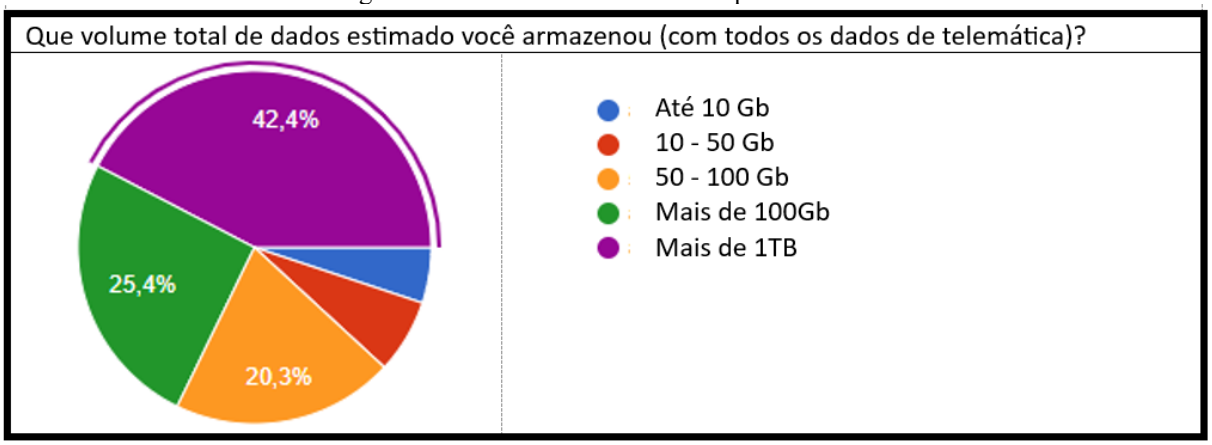
Figura 15 - Armazenamento de outros dados



Fonte: O autor (2022).

Em relação ao volume, cerca de 42% dos entrevistados informaram volume armazenado superior a 1Tb e 25% acima de 100 Gb (Figura 16).

Figura 16 - Volume armazenado - Superior a 1 Tb



Fonte: O autor (2022)

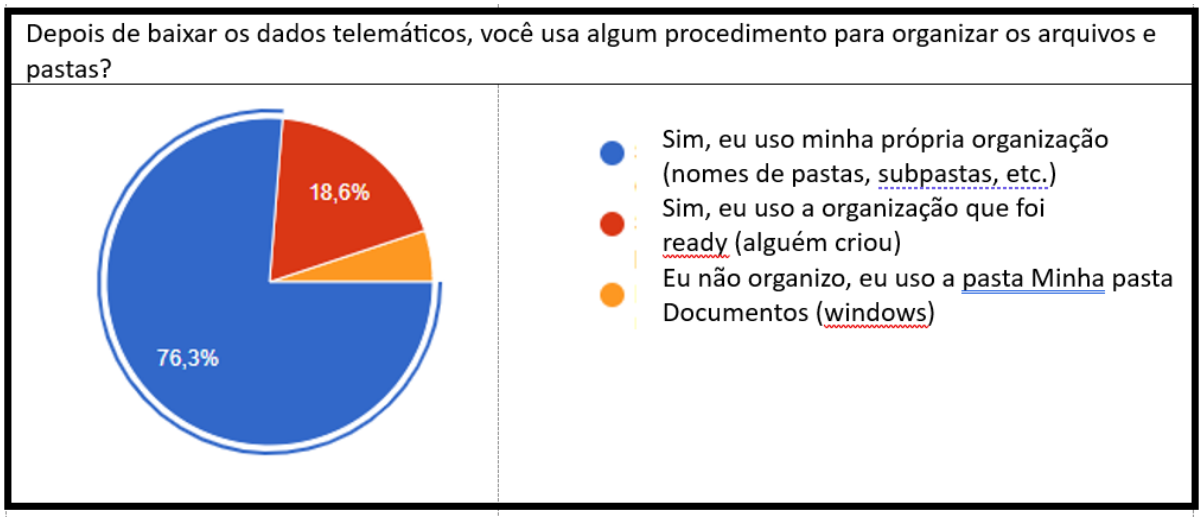
De imediato, temos o cenário problema de armazenamento pulverizado em dispositivos locais individuais e dispersos em vários ambientes, tornando praticamente impossível a gestão e o arquivamento digital adequado destes dados, além de alto risco de comprometimento da cadeia de custódia das evidências.

6.1.2 Organização dos arquivos (arquivamento digital)

A pesquisa diagnóstica preliminar apontou para um percentual de cerca de 76% de uso de organização individual (método de arquivamento próprio), 18% no uso de arquivamento já existente e os demais sem nenhuma metodologia de arquivamento, deixando os arquivos nas pastas padrões do sistema – Meus Documentos (Figura 17).

Os arquivos armazenados precisam de um mínimo de padronização no arquivamento para uma posterior recuperação da informação. Caso cada investigador use sua organização (arquivamento digital) própria, é possível que haja divergências numa busca local de informações, como duplicações, pastas e diretórios diferentes e principalmente em estações de trabalhos ou dispositivos de armazenamentos diferentes. Esse resultado nos direciona a um ambiente de dados completamente sem padronização e de difícil recuperação da informação.

Figura 17 - Principal meio de organização dos arquivos



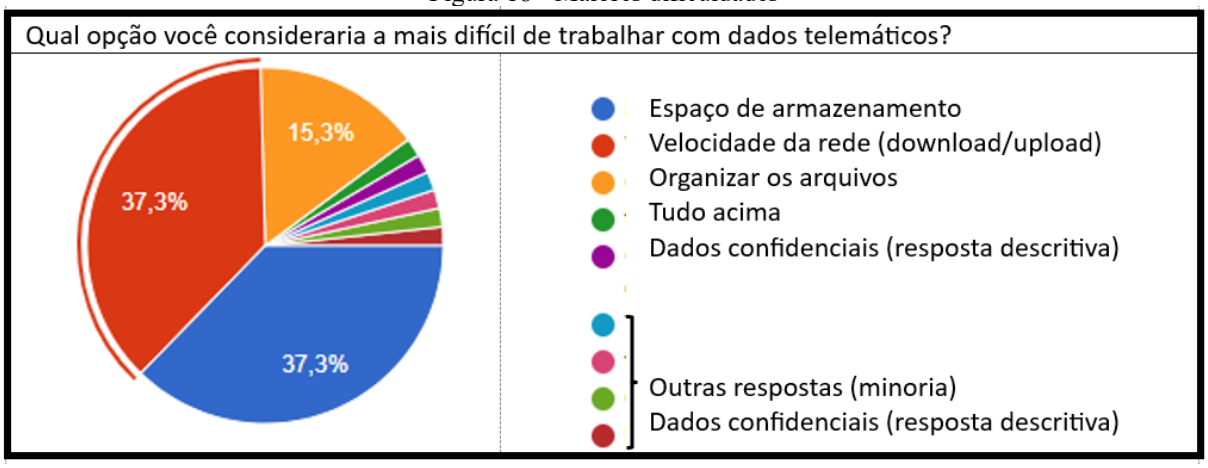
Fonte: O autor (2022)

6.1.3 Velocidade Interna da Rede

Embora exista uma robusta estrutura de rede na Polícia Federal, a demanda e o tráfego dos dados em rede nacional afetam diretamente a velocidade de *download* de forma diferente em todo o país, impactando no trabalho de obtenção (coleta) dos dados das empresas de tecnologia por meio desta rede. Não obstante, o risco de um *download* incompleto ou corrompido é possível e exigiria o reinício de todo o trabalho. A pesquisa diagnóstica preliminar

apontou como causa da principal dificuldade em trabalhar com quebra de sigilo telemático estão a velocidade de rede e o espaço de armazenamento com cerca 37% em ambas as respostas (Figura 17).

Figura 18 - Maiores dificuldades



Fonte: O autor (2022)

Observamos em terceiro lugar, com cerca de 15%, a dificuldade com a organização (arquivamento digital) foi apontada como sendo a maior dificuldade dos investigadores.

7 MODELO SUGERIDO COMO SOLUÇÃO

A criação de uma ferramenta tecnológica para gerir esse cenário não só resolveria o problema, como aumentaria em larga escala a produtividade com esse tipo de trabalho.

Com efeito, reunindo as informações de toda a pesquisa realizada e com apoio técnico de um especialista em desenvolvimento de sistemas, foi construído um protótipo preliminar do sistema, a fim de ilustrar e facilitar a visualização de uma possível construção da plataforma. Como inicialmente esclarecido no escopo deste trabalho, o desenvolvimento específico e individual da solução final não cabe aqui, sobretudo devido ao alcance e envolvimento interinstitucionais. Cada órgão possui políticas próprias na elaboração de suas plataformas corporativas, e a integração e o uso de uma plataforma comum exigiria um mínimo de consenso para a manutenção de compatibilidade e usabilidade entre todos, mantendo principalmente uma mínima integração com os sistemas e plataformas já existentes. Além disso, segundo as diretrizes do serviço público brasileiro, um sistema dessa magnitude exigiria diversos requisitos

para uma licitação, documentações técnicas, contratos de manutenção e equipes de desenvolvimento.

Desta forma, concluímos que qualquer tentativa de criação de uma versão preliminar completa desse sistema poderia ser ineficaz e possivelmente não aproveitada no serviço público e órgãos envolvidos, exigindo um retrabalho dentro daquele ambiente corporativo.

Como produto desta pesquisa, oferecemos um *framework* básico da arquitetura em camadas da plataforma, acompanhado de um diagrama de histórias de usuários e suas regras de negócio correspondentes, visando à metodologia de desenvolvimento ágil. Direcionamos, desta forma, para uma filosofia tipo MVP[34], objetivando construir uma versão mais simples e enxuta da proposta, empregando o mínimo possível de recursos para entregar a principal proposta de valor da ideia. São elementos suficientes para o desenvolvimento final da solução pretendida em qualquer ambiente.

7.1 A PLATAFORMA – ESC (*EVIDENCE SECURE CHAIN*)

Um protótipo de demonstração com um *Web Frontend*[35] foi elaborado com intuito de ilustrar o fluxo mínimo do processo e as telas do sistema, e direcionar o desenvolvimento corporativo da versão operacional, segundo as políticas da instituição. O nome do sistema foi definido como **ESC**, acrônimo de *Evidence Secure Chain.* Com o apoio de outro servidor da instituição, especialista em programação e desenvolvimento de *software*, um protótipo preliminar foi desenvolvido inicialmente sem a tecnologia *Blockchain*. Descrevemos a seguir algumas características utilizadas nesta interface gráfica do sistema.

***Front-end* com HTML, JavaScript e CSS**

- Uso de recursos HTML5, com as validações cliente e *feedbacks* de validações do servidor;
- Conteúdo de CSS puro com alguns componentes do *Bootstrap*, na interface de navegação;
- Aplicativo de página única usando JavaScript sem estrutura de *front-end* (será substituído pelo React em versões futuras);

[34] MVP - sigla em inglês para *minimum viable product* – ou produto mínimo viável. Em empreendedorismo, principalmente no contexto de *startups*, um produto viável mínimo é a versão mais simples de um produto que pode ser lançada com uma quantidade mínima de esforço e desenvolvimento.
[35] *Web Front-End* - é a interface gráfica do usuário de um *site* ou *software*.

***Back-end* com Python, Django, Django REST e Simple JWT**

- API REST usando exibições herdadas diretamente de rest_framework.views.APIView
- *Django* Puro ORM, com migrações. Precisa de melhorias futuras com a criação de índices.

***PostgreSQL* para acesso a banco de dados relacional**

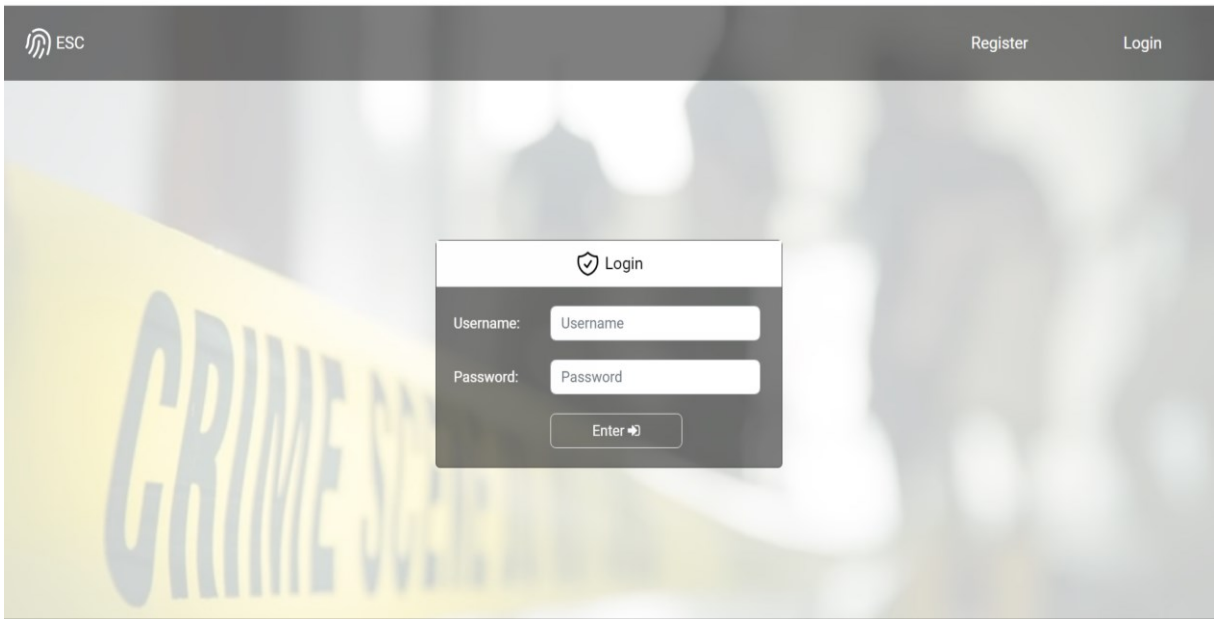
As características acima descritas possivelmente seriam alteradas e/ou ajustadas conforme consenso de utilização entre os *stakeholders.*[36] Neste primeiro momento, apenas ilustramos com algumas possibilidades, sabendo que no ambiente corporativo e institucional, com a escalabilidade e alta demanda, muitas dessas características possivelmente serão readequadas.

7.1.1 Tela de *login* do sistema

O *layout* inicial da tela do sistema é o apresentado na figura abaixo (Figura 17). Na primeira tela, o usuário credenciado se conecta ao sistema com suas credenciais, cria caso e/ou concede acesso a um provedor de serviços, que por meio de ordem judicial irá fornecer os dados de interesse.

[36] *Stakeholder* é um dos termos utilizados em diversas áreas como gestão de projetos, comunicação social administração e arquitetura de *software* referente às partes interessadas que devem estar de acordo com as práticas de governança corporativa executadas pela empresa ou instituição. No caso em tela, as instituições envolvidas na persecução criminal.

Figura 19 - Tela de *login* do sistema ESC



Fonte: O autor (2023).

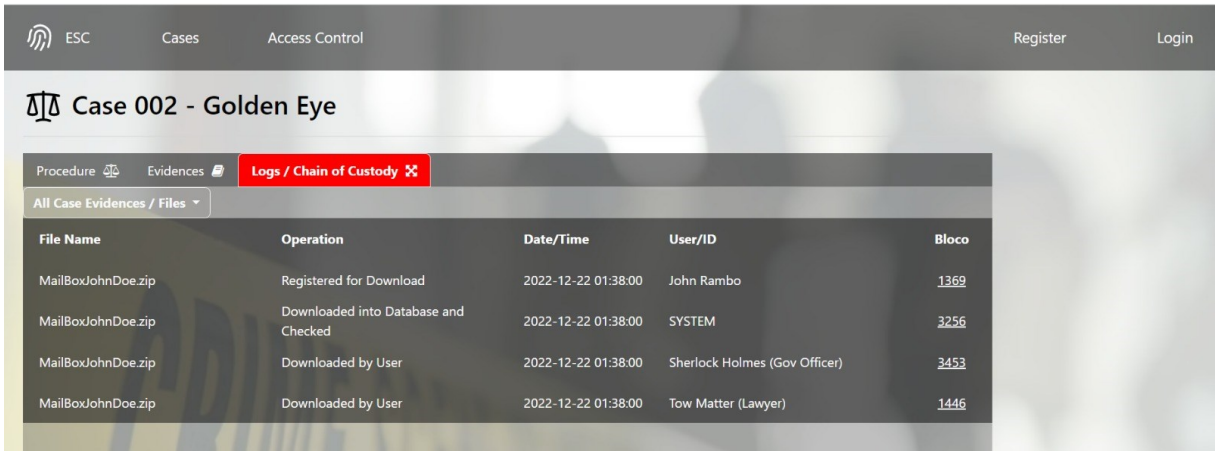
Na etapa seguinte, o sistema se conecta ao sistema com suas credenciais, por meio de uma API[37] (*Application Programming Interface* ou interface de programação de aplicação) e acessa o caso; faz *upload* dos dados, informando o *hash*. O sistema recebe o arquivo e já valida o *hash*, indicando isso no *status* da evidência.

7.1.2 Tela de visualização das interações com as evidências – *logs*

Nas etapas seguintes, seguem os demais interessados envolvidos no trato com as evidências adquiridas. Durante todo o processo, um *log* de registros armazena os detalhes dos envolvidos na cadeia de custódia, como vemos na Figura 18.

Figura 20 - Registros de acessos ao sistema

[37] API significa *Application Programming Interface* (interface de programação de aplicação). No contexto de APIs, a palavra "aplicação" refere-se a qualquer *software* com uma função distinta. A interface pode ser pensada como um contrato de serviço entre aplicações.



Fonte: O autor (2023)

Nesta tela de registros das interações com a evidência, podemos observar os registros de carimbos de tempo, nome do arquivo e identificação dos usuários que tiveram contato com o referido dado. Neste ponto, o registro e o controle de todas essas interações serão registrados em uma *Blockchain* de consórcio, cujas características garantirão o controle no manuseio, a transparência e autenticidade das evidências trabalhadas.

7.1.3 O arquivamento digital dos dados

Como mencionado, a organização dos arquivos, do conhecimento ou da informação não foi foco deste trabalho, tendo sido apenas definida como pressuposto uma organização mínima para o arquivamento, de forma a evitar a dispersão dos dados, por meio de organização digital em pastas com o mínimo de informações para sua recuperação.

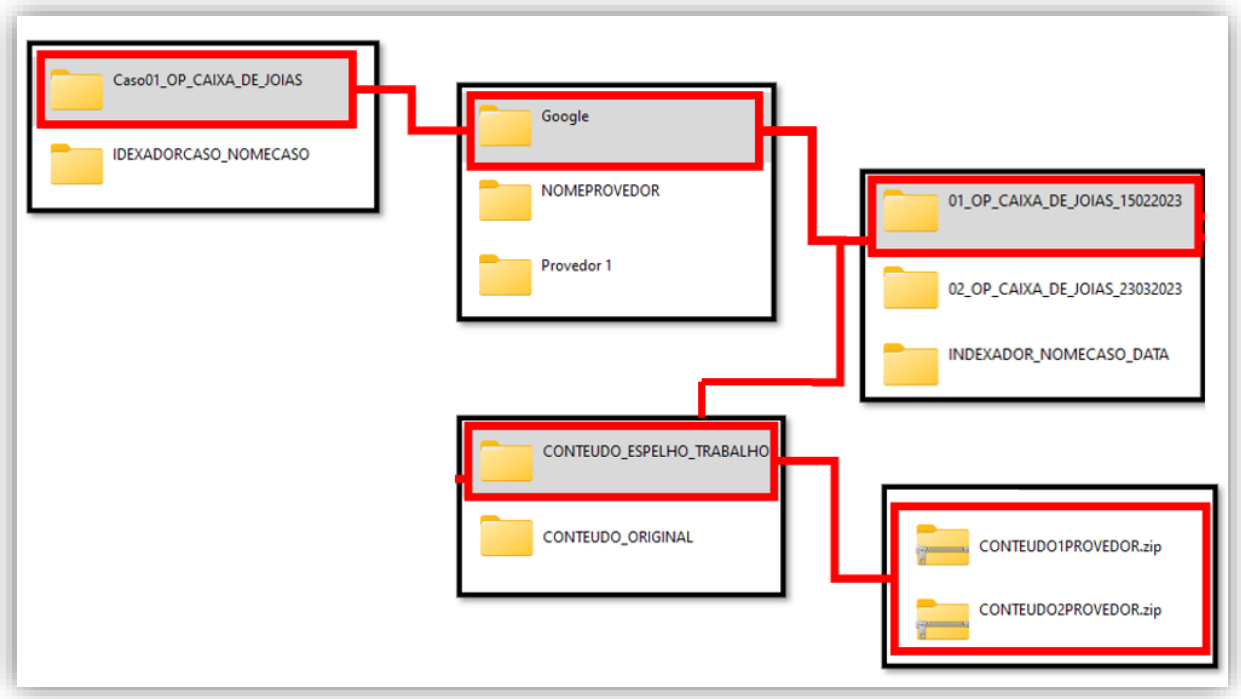
Segundo Pajeú *et al.* (2018), a codificação é uma parte física do processo de classificação que visa à adoção de um método de arquivamento (alfanumérico, duplex, variadex, decimal etc.), para traduzir e aparelhar a estrutura hierárquica, facilitando as atividades de classificação. Resulta na escolha de algum símbolo que facilite a localização dos fundos, séries e subséries de documentos dentro do acervo.

Conforme descrito por Sousa (2009), a etapa básica do arquivamento foi realizada como a prática de acondicionar e armazenar os documentos em pastas ou caixas, obedecendo à ordenação definida pelo esquema de classificação, sendo este trabalho realizado no acondicionamento em pastas digitais.

Para isso, sugerimos alguns padrões de nomeação de pastas e arquivos tomados como referência no manual de boas práticas para gestão de pastas e arquivos digitais, elaborado pelo Serviço de Gestão do Conhecimento do Tribunal de Contas da União (BRASIL-TCU, 2019).

a) Para possibilitar precisão na recuperação de arquivos e pastas, recomenda-se não utilizar caracteres especiais, tais como“&”,“#”, vírgulas, parênteses e letras acentuadas.
b) Outro fator que auxilia na recuperação de arquivos e pastas é a utilização de hífen ou *underscore* para separar cada palavra contida no nome. Recomenda-se uso de hífen, pois este não “desaparece” quando apresentado sob a forma de *link*.
c) As pastas devem ser nomeadas com um indexador e nome do caso cadastrado na plataforma, INDEXADOR_NOMEDOCASO, imediatamente seguidos por subpasta com o nome do provedor, NOMEDOPREOVEDOR, seguido de outra subpasta contendo um indexador, nome do caso e data, INDEXADOR_NOMEDOCASO_DATA, seguido de outras duas subpastas contendo o conteúdo original e outra pra o manuseio dos dados e, por fim, o conteúdo do provedor (Figura 19).

Figura 21 - Exemplo arquivamento digital - Pastas



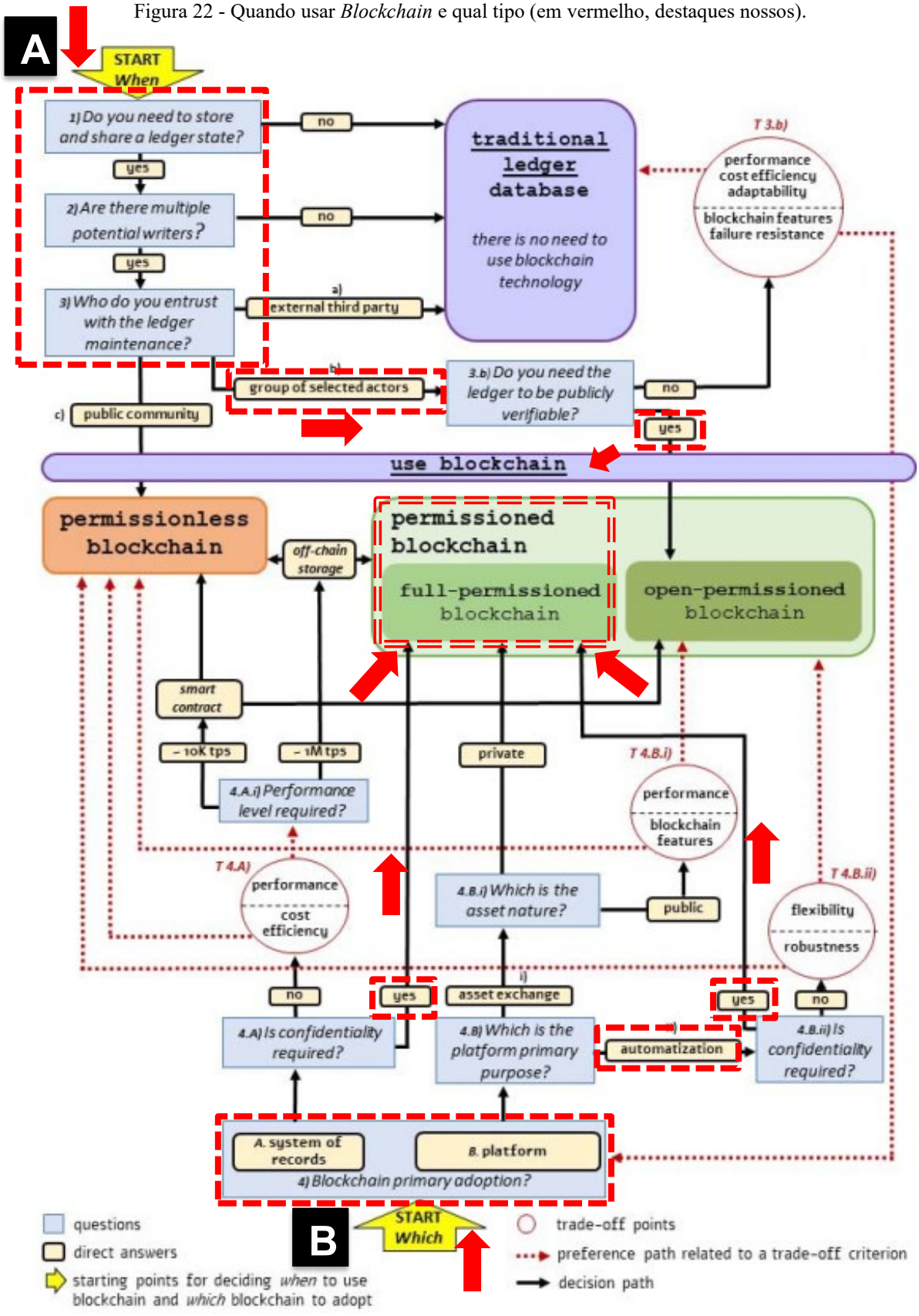
Fonte: Elaborado pelo autor (2023).

7.1.4 A camada *Blockchain*

Os trabalhos aqui estudados apontaram para a utilização de uma *Blockchain* privada ou de consórcio. E de acordo com as premissas do trabalho com as evidências digitais e seus atores envolvidos, já descritos neste trabalho, acreditamos ser a escolha correta.

Entretanto, buscamos maior sustentação dessa ideia em um trabalho técnico bem aprofundado sobre o tema, *A Vademecum on Blockchain Technologies: When, Which, and How*, um compilado de mais de 300 artigos técnicos sobre o tema. No trabalho em questão, Belotti (2019) apresenta um diagrama para escolha ou não do uso da tecnologia *Blockchain* e seleção do tipo mais adequado, o qual reproduzimos abaixo, com destaques nossos, para os propósitos desta pesquisa.

Figura 22 - Quando usar *Blockchain* e qual tipo (em vermelho, destaques nossos).



Fonte: BELOTTI, 2019.

O diagrama acima (Figura 20) nos direciona claramente para o uso de uma *Blockchain* totalmente permissionada.

Nas três primeiras decisões a serem tomadas (ponto A destacar), é necessário saber se precisamos armazenar e compartilhar o estado de um livro-razão, se existem outros participantes a escrever registros na rede e se a manutenção da rede será pública ou por um grupo de participantes: a resposta a todas elas é "sim". Todos os envolvidos na persecução criminal irão compartilhar e participar na escrita de registros, bem como serão os responsáveis pela manutenção.

Avançando nos questionamentos, chegamos à decisão da necessidade de que o livro-razão seja publicamente verificável e a resposta é "certamente que sim". Concluindo a primeira etapa, é necessário o uso de uma rede *Blockchain.*

No segundo momento (ponto B destacado), será necessário avaliar que tipo de rede seria adequada. Num primeiro questionamento se a adoção primária será para um sistema de registros ou uma plataforma para automatização, temos que avaliar se a confidencialidade seria um requisito e, no caso em questão, a resposta é positiva. Sendo assim, em ambas as situações para um sistema de registros ou plataforma para automatização, somos direcionados a uma rede *Blockchain* totalmente permissionada.

Este resultado corrobora os trabalhos relacionados, nos quais a maioria dos pesquisadores apontaram em seus artigos uma rede *Blockchain* de consórcio, uma rede totalmente permissionada com a participação de membros autorizados. Assim, concluímos que possivelmente seria a proposta mais adequada para uso no caso deste trabalho.

7.1.5 O armazenamento

Soluções de armazenamento baseadas em um sistema de arquivos distribuídos estão crescendo ainda mais rápido, em números e capacidade de implementações. O motivo: crescimento acentuado e contínuo em dados não estruturados em *data centers* empresariais. Dobrando os volumes de dados não estruturados a cada ano, as organizações estão ligando os sistemas de arquivos distribuídos para gerenciar volumes de dados com maior desempenho, facilidade operacional aprimorada e custos menores (DELL, 2023).

Consideramos que, em virtude de a maioria dos dados oriundos das fontes tecnológicas serem não estruturados e de grande volume, um armazenamento do tipo distribuído seria possivelmente o mais adequado. Entretanto, não faz parte do escopo deste trabalho a pesquisa

ou definição do melhor armazenamento a ser utilizado com a arquitetura proposta. As instituições envolvidas no processo (empresas de tecnologia, polícia, Ministério Público, Judiciário, Defesa – OAB) precisam inicialmente concordar, em termos gerais, como serão definidos os armazenamentos dessas evidências digitais, considerando a segurança dos dados, as características dos armazenando já existente nessas instituições e a disponibilidade para todos os membros participantes desse consórcio. A garantia da autenticidade e os registros do manuseio da evidência por qualquer participante serão garantidos pela rede *Blockchain*.

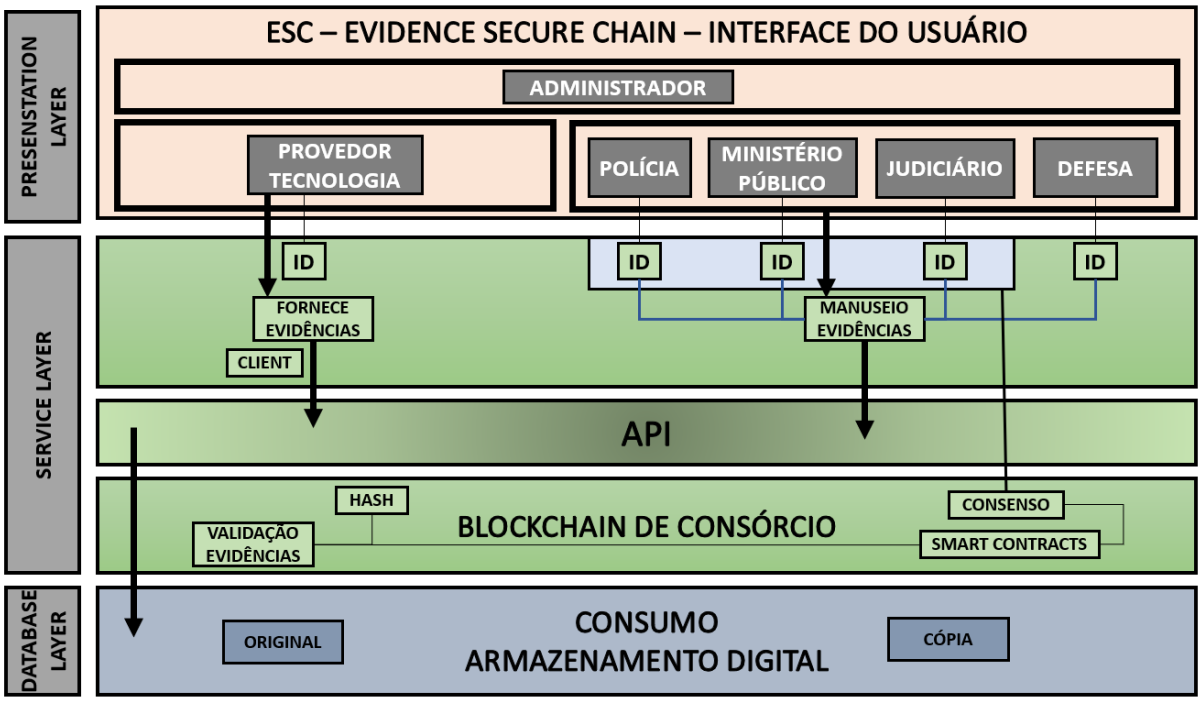
7.1.6 Arquitetura – *framework* em camadas do sistema

Existem diversos padrões arquiteturais, mas exemplificaremos com um relativamente comum (arquitetura em camadas), até porque não existe um funcionamento padrão ou preestabelecido para todos os sistemas. Tudo depende da necessidade do negócio e do tipo da solução.

O padrão de arquitetura mais comum é o *layered pattern,* ou padrão de arquitetura em camadas, também conhecido como padrão de arquitetura de *n* camadas. Esse é o padrão de fato para a maioria dos aplicativos Java EE e, portanto, é amplamente conhecido pela maioria dos arquitetos, *designers* e desenvolvedores. O padrão de arquitetura em camadas se aproxima da comunicação tradicional de TI e das estruturas organizacionais encontradas na maioria das empresas, o que o torna uma escolha natural para a maioria dos esforços de desenvolvimento de aplicativos de negócios. Os componentes dentro do padrão de arquitetura em camadas são organizados em camadas horizontais, cada qual desempenhando uma função específica dentro do aplicativo (por exemplo, lógica de apresentação ou lógica de negócios). Cada camada do padrão de arquitetura em camadas tem uma função e responsabilidade específicas dentro do aplicativo. Por exemplo, uma camada de apresentação seria responsável por lidar com toda a lógica de comunicação da interface do usuário e do navegador, enquanto uma camada de negócios seria responsável por executar regras de negócios específicas associadas à solicitação. (RICHARDS, 2015).

Na sequência, esboçamos uma arquitetura hierárquica básica em camadas para descrever o sistema (Figura 21).

Figura 23 - Arquitetura hierárquica em três camadas



Fonte: O autor (2023)

A primeira camada trata da interface de interação dos usuários e permite acesso à plataforma por meio de autenticação dos usuários e administradores do sistema, que poderão interagir com a plataforma através da Internet. Por meio da interface, será possível interagir com a rede *Blockchain* por meio da API, para unicamente visualizar os registros referentes às evidências e todas as suas interações. A API promove integração entre as camadas e suporte entre si para atender aos requisitos da plataforma. Também por esta camada, o usuário poderá solicitar, visualizar e obter os dados junto ao provedor, além de verificar os registros de acesso em todo o processo de obtenção dos dados e todos os envolvidos.

Na segunda camada, temos os serviços envolvidos, uma subcamada de gestão do sistema, outra com a automação para conexão ao provedor de dados e uma última com a *Blockchain*.

Na subcamada de gestão e serviços, temos a gestão de usuários por um perfil administrador, que define os acessos e permissões de cada usuário e sua identidade (ID), promove a integração por meio da API com subcamada de *Blockchain,* permitindo os registros dos dados e validação dos blocos, bem como a visualização dos registros conforme a permissão de cada usuário.

Na subcamada da interface de aplicação (API), temos a integração direta com os provedores de dados, que se comunicam com o sistema por meio do serviço de cliente (API *client*), fornecendo os dados requisitados. Por meio desta camada, também será possível realizar o arquivamento digital dos arquivos fornecidos no repositório de dados.

A subcamada da rede *Blockchain* tem por finalidade prover confiabilidade, transparência, imutabilidade e facilidade de verificação dos dados de quebra de sigilo telemático autorizados judicialmente e todos os registros atrelados ao caso agora registrados na rede. A camada da rede *Blockchain* é separada da camada de armazenamento, separando o armazenamento do gerenciamento de evidências, garantindo melhor escalabilidade, além de ser integrada à API, que tem o papel de integrar todas as etapas. Nesta camada, por meio de contratos inteligentes, poderão ser recebidos os arquivos conforme requisição do usuário e validados em consenso pelos participantes autorizados. Todas as interações com usuários e todos os processos são validados e registrados com carimbo de tempo nos blocos, que podem ser consultados pela interface gráfica.

Na terceira camada, temos o armazenamento, onde ficarão os dados originais fornecidos e uma cópia, garantindo a autenticidade dos dados originais, para disponibilização aos interessados, e *softwares* de análise de evidências digitais. O armazenamento possivelmente distribuído será mais bem especificado conforme a necessidade e a infraestrutura já existentes entre os participantes.

7.1.7 Histórias de usuários e regras do negócio

Um componente-chave do desenvolvimento ágil de *software*[38] (*Agile Software Development – ASD*) é colocar as pessoas em primeiro lugar, e uma história de usuário coloca os usuários finais no centro da conversa. Essas histórias usam linguagem não técnica para fornecer contexto para a equipe de desenvolvimento e seus esforços. Depois de ler uma história de usuário, a equipe sabe por que está construindo, o que está construindo e que valor isso cria.

[38] Desenvolvimento Ágil é uma abordagem que utiliza processos e práticas que promovem a entrega contínua de software de qualidade, ajustando-se rapidamente a mudanças de requisitos ao longo do ciclo de desenvolvimento. **Fonte**: BECK, Kent et al. Manifesto for Agile Software Development. 2001. Disponível em: https://agilemanifesto.org/.

Uma história de usuário (*user story mapping*) é uma explicação geral e informal de um recurso de *software* escrito a partir da perspectiva do usuário final. Seu objetivo é articular como um recurso de *software* fornecerá valor ao cliente (PATTON, 2014).

Segundo Alhazmi *et al.* (2020), uma história de usuário é a menor unidade de trabalho na estrutura do *Scrum*[39] e é um objetivo final, não um recurso. A equipe construirá os protótipos com base nas histórias do usuário, levando em consideração os relacionamentos entre as histórias do usuário e suas regras de negócios.

Para cada história de usuário, existem detalhes específicos ou condições, normalmente relacionadas em regras de negócio ou de escopo funcional. Estas são padrões que condicionam o funcionamento do negócio, sendo comumente aplicadas no contexto da arquitetura de *softwares*.

Desta forma, apresentam-se no apêndice A, ao final deste trabalho, de forma resumida e simplificada, as histórias de usuários envolvidas na ideia proposta, juntamente com algumas regras de negócio, as premissas básicas e funcionais para o funcionamento da ideia proposta, facilitando assim o desenvolvimento da arquitetura sugerida. E de forma resumida, apresentamos abaixo, no quadro 3, as histórias descritas.

Quadro 3 - Histórias de usuários - tabela resumo

ID DE HISTÓRIA DO USUÁRIO	COMO O <tipo de usuário>	QUER <premissa de tarefas>	PARA QUE POSSA <realizar algum objetivo>
1	Administrador	1-Logar no sistema. 2-Cadastrar usuários e definir permissões de acesso. 3-Definir membros participantes da validação dos dados. 4-	1-Para entrar na plataforma. 2-Para autorizar e delimitar acesso aos usuários do sistema. 3- Para que a camada blockchain realize o consenso validação com segurança. 4-
2	Investigador	1-Logar no sistema. 2-Cadastrar caso de quebra de dados. 3-Fazer upload de ordem judicial. 4-Gerenciar casos e evidências permitidos. 5-Fazer download de evidências. 6- Visualizar histórico dos registros de manuseio da evidência e do processo de obtenção dos dados.	1-Para entrar na plataforma. 2-Para solicitar e receber quebra de dados. 3- Para solicitar e receber quebra de dados. 4- Para acessar e visualizar casos e evidências permitidos. 5- Para obter dados de quebra. 6- Para realizar auditoria no processo de quebra e verificar a integridade dos dados e de todo o procedimento.

[39] *Scrum* é um *framework* de gerenciamento que as equipes usam para se auto-organizar e trabalhar em direção a um objetivo em comum. A estrutura descreve um conjunto de reuniões, ferramentas e funções para uma entrega eficiente de projetos.

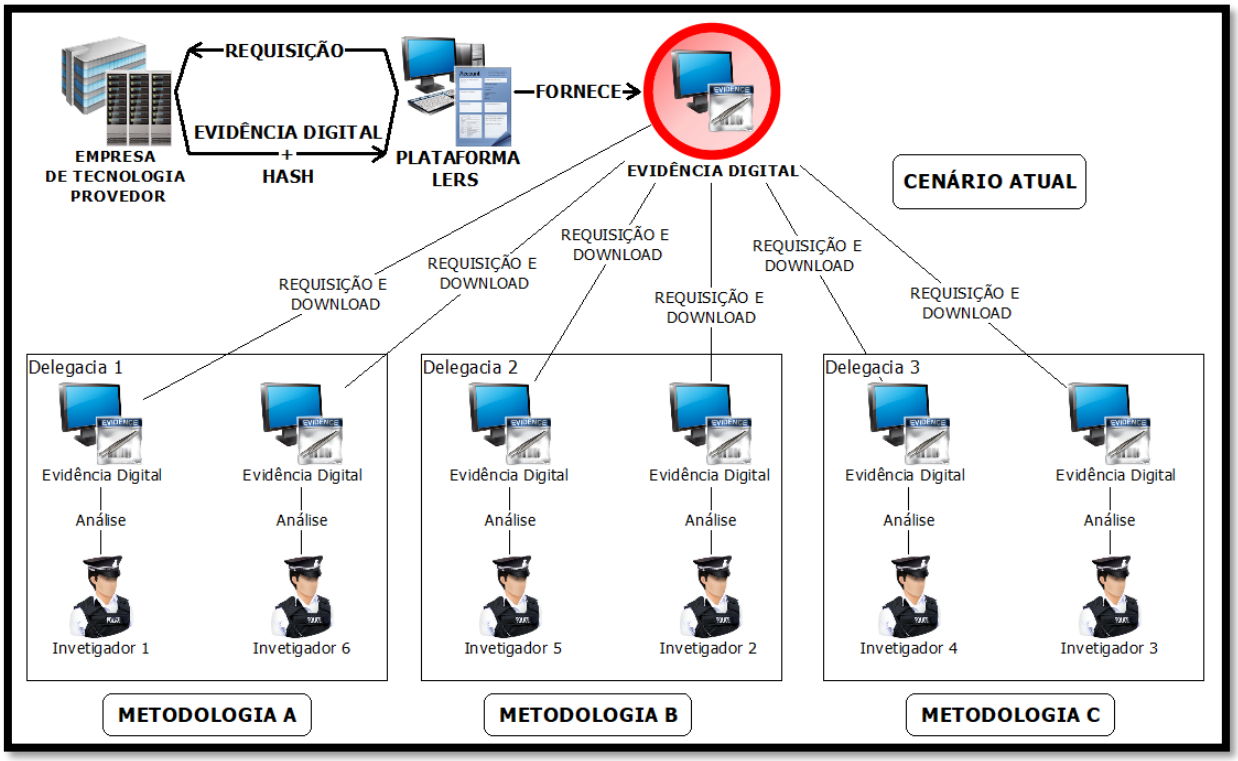
3	Provedor	1-Logar no sistema via API *client* ou pela plataforma. 2- Fazer download de ordem judicial e cumprir ordem judicial. 3-Fornecer garantia de autenticidade por meio de *hash* dos arquivos.	1- Para entrar na plataforma. 2-Fazer upload de dados da quebra autorizados em ordem. 3-Para garantir a segurança, autenticidade e validade do processo de envio de dados.
4	Judiciário	1-Logar no sistema. 2-Cadastrar caso de quebra de dados. 3-Fazer upload de ordem judicial. 4-Gerenciar casos e evidências permitidos. 5-Fazer download de evidências. 6- Visualizar histórico dos registros de manuseio da evidência e do processo de obtenção dos dados.	1-Para entrar na plataforma. 2-Para solicitar e receber quebra de dados. 3- Para solicitar e receber quebra de dados. 4- Para acessar e visualizar casos e evidências permitidos. 5- Para obter dados de quebra. 6- Para realizar auditoria no processo de quebra e verificar a integridade dos dados e de todo o procedimento.
5	Ministério Público	1-Logar no sistema. 2-Cadastrar caso de quebra de dados. 3-Fazer upload de ordem judicial. 4-Gerenciar casos e evidências permitidos. 5-Fazer download de evidências. 6- Visualizar histórico dos registros de manuseio da evidência e do processo de obtenção dos dados.	1-Para entrar na plataforma. 2-Para solicitar e receber quebra de dados. 3- Para solicitar e receber quebra de dados. 4- Para acessar e visualizar casos e evidências permitidos. 5- Para obter dados de quebra. 6- Para realizar auditoria no processo de quebra e verificar a integridade dos dados e de todo o procedimento.
6	Defesa	1-Logar no sistema. 2-Fazer download de ordem judicial. 3-Gerenciar casos e evidências permitidos. 4-Fazer download de evidências. 5- Visualizar histórico dos registros de manuseio da evidência e do processo de obtenção dos dados.	1-Para entrar na plataforma. 2- Para verificar autenticidade e validade da quebra de dados. 3- Visualizar casos e evidências permitidos. 4- Para obter dados de quebra. 5- Para realizar auditoria no processo de quebra e verificar a integridade dos dados e de todo o procedimento.
7	API	1-Logar no sistema. 2-Cadastrar caso de quebra de dados. 3-Gerenciar casos e evidências permitidos. 4-Fazer download de evidências. 5- Obter todas as informações e carimbos de tempo dos registros de manuseio da evidência e do processo de obtenção dos dados.	1-Para entrar na plataforma. 2-Para solicitar e receber quebra de dados. 3- Para acessar e visualizar casos e evidências permitidos. 4- Para obter dados de quebra. 5- Para registrar na *Blockchain* todas as etapas do processo de quebra e interações com as evidências digitais, garantindo a integridade dos dados e de todo o procedimento.

Fonte: O autor (2023).

8 CONCLUSÕES

A modelagem do processo e os resultados obtidos com a avaliação diagnóstica permitiram inferir conclusões que corroboram com o cenário prático do ciclo de vida das evidências digitais produzidas na quebra de sigilo telemático. Embora os procedimentos entre os profissionais de investigação sejam semelhantes, cada grupo ainda realiza tarefas de maneira não padronizada. Como resultado, a coleta (requisição e *download*) e o armazenamento dos dados seguem processos variados, com arquivos sendo organizados de formas distintas, conforme identificado na avaliação diagnóstica (Figura 24).

Figura 24 – Procedimentos similares e sem padrão



Fonte: O autor (2022)

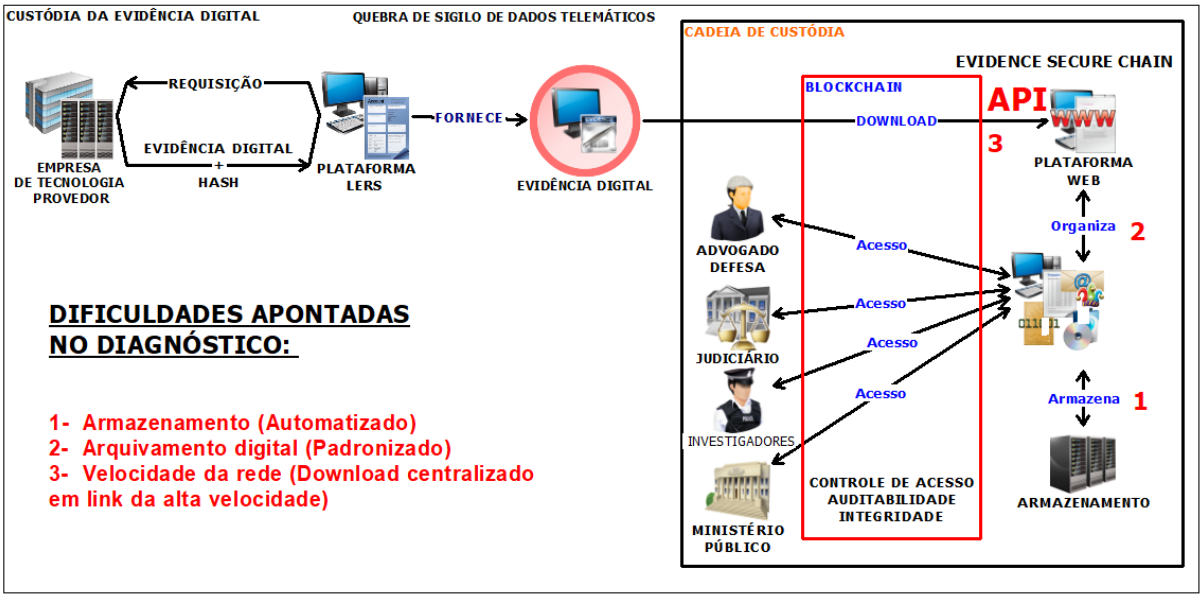
A pesquisa alcançou plenamente seus objetivos ao mapear o fluxo completo, destacando as etapas de aquisição, arquivamento digital e armazenamento dos dados. Além disso, as principais causas dos problemas foram identificadas, como a inexistência de uma metodologia padronizada e de ferramentas tecnológicas automatizadas, que se mostraram os fatores limitantes mais significativos.

As primeiras etapas concentraram-se em descrever o fluxo do processo de gestão, identificar os principais problemas e analisar suas causas. Primeiramente, o ciclo de vida das evidências digitais foi esquematizado, com foco nos dados obtidos a partir da quebra de sigilo telemático. Esse mapeamento detalhado revelou o fluxo completo, desde a requisição judicial até o armazenamento final dos dados, passando pelas etapas de aquisição, *download* e organização das evidências.

Em seguida, foram identificadas as principais fragilidades na gestão desses dados, com destaque para a ausência de uma metodologia padronizada e de ferramentas tecnológicas que automatizassem o processo. O diagnóstico apontou a gestão manual dos arquivos como um dos principais fatores que comprometem a integridade das evidências, gerando inconsistências na cadeia de custódia. A inexistência de automatização, a dependência de procedimentos manuais e a ausência de um sistema centralizado para monitoramento e arquivamento dos dados foram identificadas como as principais causas dos problemas. Essa análise evidenciou a necessidade de uma abordagem mais robusta e segura para garantir a preservação e rastreabilidade das evidências digitais.

Com base nessas análises, os últimos pontos do trabalho concentraram-se em propor uma solução automatizada para a gestão de evidências digitais e desenvolver um framework de arquitetura que suporte essa solução. Utilizando a tecnologia *blockchain*, a proposta garante a imutabilidade e rastreabilidade das evidências, eliminando as falhas associadas ao manuseio manual e assegurando que todas as interações com os dados sejam registradas de maneira inviolável. Essa abordagem padroniza o arquivamento digital, proporcionando maior segurança e eficiência na gestão das evidências ao longo de toda a cadeia de custódia (Figura 25).

Figura 25 - Arquitetura básica proposta



Fonte: O autor (2023)

Foi desenvolvido um *framework* de arquitetura para o protótipo da plataforma "*Evidence Secure Chain*" (ESC), projetada para organizar os dados de forma predefinida, facilitando o controle e garantindo a integridade dos arquivos. A ESC é uma plataforma robusta que elimina a necessidade de etapas manuais, como download, arquivamento e armazenamento, padronizando essas operações para todos os usuários. Esse *framework* estabelece uma base sólida para a futura implementação de um sistema automatizado, capaz de otimizar a gestão das evidências digitais e garantir a conformidade rigorosa com a cadeia de custódia no âmbito das investigações criminais.

Ao padronizar essas etapas, a solução proposta assegura um controle robusto sobre as interações com as evidências, preservando a imutabilidade e rastreabilidade de todas as ações relacionadas às evidências digitais. Dessa forma, o trabalho contribui significativamente para a eficiência da persecução penal, ao oferecer uma solução inovadora e padronizada para a gestão de dados telemáticos, atingindo com sucesso os objetivos estabelecidos.

9 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo geral propor uma solução automatizada para a gestão da cadeia de custódia dos dados telemáticos obtidos judicialmente na investigação criminal brasileira, utilizando a tecnologia *blockchain* para garantir a imutabilidade e rastreabilidade das evidências digitais. Todos os objetivos específicos propostos foram plenamente alcançados.

O fluxo do processo de gestão dos dados telemáticos foi descrito e mapeado de maneira detalhada, revelando as principais etapas de aquisição, arquivamento digital e armazenamento. Durante a análise, foram identificadas as principais fragilidades, como a inexistência de uma padronização e a ausência de ferramentas automatizadas, destacando a necessidade de melhorias significativas na gestão dessas evidências. A partir dessa análise, foi proposta uma solução inovadora, baseada na tecnologia *blockchain*, para garantir a integridade e a segurança dos dados, eliminando as vulnerabilidades relacionadas ao manuseio manual e assegurando a imutabilidade das evidências.

Para implementar essa solução, foi desenvolvido o *framework* de arquitetura de um protótipo da plataforma "Evidence Secure Chain" (ESC), que padroniza o processo de gestão dos dados telemáticos, proporcionando um ambiente seguro e eficiente para o controle das evidências digitais.

Embora os resultados deste trabalho tenham atingido todos os objetivos propostos, há campos a serem explorados por futuros estudos. Entre eles, destacam-se o tipo ideal de armazenamento, que pode garantir maior eficiência e segurança no tratamento dos dados, e a organização da informação para facilitar a recuperação inteligente dos dados. Além disso, o uso de inteligência artificial (IA) dentro da plataforma apresenta-se como uma oportunidade promissora com várias possibilidades. A integração dessa solução com os sistemas já existentes nas instituições investigativas são também áreas que merecem atenção de futuros pesquisadores, ampliando o impacto e a aplicabilidade da solução proposta.

Este trabalho consolidou-se com a publicação de um capítulo no Advanced Notes in Information Science, v. 4, 2023 (https://doi.org/10.47909/anis.%20978-9916-9906-3-6.65) e com a apresentação no **I Seminário de Ciência da Informação e Suas Conexões com a Ciência Policial - PGCIN/UFSC** (https://www.youtube.com/watch?v=qreCmp6tlUE), realizado em 29/09/2023. Além disso, foi submetido ao periódico *Information Sciences – Journal* e está em fase de revisão editorial.

10 REFERÊNCIAS

AGARWAL, Ritu; DHAR, Vasant. Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research. **Published Online**, 25 Sep 2014.

AHMAD, Liza et al. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In: **Proceedings of the 15th international conference on availability, reliability and security**. 2020. p. 1-8.

ALHAZMI, Alhejab; HUANG, Shihong. Integrating design thinking into scrum framework in the context of requirements engineering management. In: **Proceedings of the 3rd International Conference on Computer Science and Software Engineering**. 2020. p. 33-45.

ANNE, Venkata Praveen Krishna *et al*. Storing and Securing the Digital Evidence in the Process of Digital Forensics through *Blockchain* Technology. In: **Proceedings of the International Conference on Data Science, Machine Learning and Artificial Intelligence.** 2021. p. 272-276.

ARANTES JUNIOR, Gladstone. *Blockchain*: confiança em transações públicas e o caso do BNDES. 2018. Disponível em: <https://web.bndes.gov.br/bib/jspui/bitstream/1408/18820/1/PRArt214865_Blockchain%20e%20o%20caso%20do%20BNDES_14-21_P.pdf>. Acesso em: 02 abr. 2023.

ARANTES JUNIOR, Gladstone. *Rede Blockchain Brasil*. Repositório de arquivos para a infraestrutura da Rede Blockchain Brasil. 2021. Disponível em: <https://github.com/RBBNet/rbb>. Acesso em: 02 abr. 2023.

BARTH, Fabricio J. *et al*. Recuperação e mineração de informações para a área criminal. **ENIA VI-Encontro Nacional de Inteligência Artificial. Anais do XXVII Congresso da SBC**, p. 1292-1301, 2007.

BELOTTI, Marianna *et al*. A vademecum on *Blockchain* technologies: When, which, and how. **IEEE Communications Surveys & Tutorials**, v. 21, n. 4, p. 3796-3838, 2019.

BONOMI, Silvia; CASINI, Marco; CICCOTELLI, Claudio. B-coc: A *Blockchain* -based chain of custody for evidence management in digital forensics. **arXiv preprint arXiv**:1807.10359, 2018.

BORRI, Luiz Antonio; DE ÁVILA, Gustavo Noronha. A cadeia de custódia da prova no "Projeto de Lei Anticrime": suas repercussões em um contexto de encarceramento em massa. **Direito Público**, v. 16, n. 89, 2019.

BORKO, Harold. Ciência da Informação: o que é isto. **American Documentation**, v. 19, n. 1, p. 1-2, 1968.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**, Presidência da República. Casa Civil - Subchefia para Assuntos Jurídicos, Brasil,1941. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em: 10 dez. 2022.

BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal**. Brasil, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 10 dez. 2022.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. **Pacote Anticrime**. Brasil, 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 10 dez. 2022.

BRASIL. Decreto-lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasil, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2022.

BRASIL. TCU – Tribunal de Contas da União. **Levantamento da tecnologia *Blockchain*** / Tribunal de Contas da União; Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria das Sessões (Seses), 202039 p.: il. – (Sumário Executivo e apêndices), 2018. Disponível em: https://portal.tcu.gov.br/levantamento-da-tecnologia-*Blockchain*.htm. Acesso em: 10 dez. 2022.

BRASIL. TCU – Tribunal de Contas da União. **Manual de Boas Práticas para Gestão de Pastas e Arquivos Digitais.** Instituto Serzedello Corrêa. Centro de Documentação. Serviço de Gestão do Conhecimento. 2019. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A81881F701C7A860170634744F16480&sa=U&ved=2ahUKEwiYk421g-b9AhWdq5UCHWAXCmIQFnoECAkQAQ&usg=AOvVaw0m0j3bcEwCLYeTYGjcGt6D>. Acesso em: 10 jan. 2023.

BURRI, Xavier et al. Chronological independently verifiable electronic chain of custody ledger using blockchain technology. **Forensic Science International: Digital Investigation**, v. 33, p. 300976, 2020.

CASTRO, Miguel; LISKOV, Barbara. Practical Byzantine fault tolerance and proactive recovery. **ACM Transactions on Computer Systems (TOCS)**, v. 20, n. 4, p. 398-461, 2002.

CHEN, Hsinchun; CHIANG, Roger H. L.; STOREY, Veda C. Business intelligence and analytics: From big data to big impact. **MIS quarterly**, p. 1165-1188, 2012.

CHOPADE, Mrunali et al. Digital forensics: Maintaining chain of custody using *Blockchain.* In: **2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE**, 2019. p. 744-747.

CHRISTENSEN, C. M. O dilema da inovação: Quando as novas tecnologias levam empresas ao fracasso. Brasil: M. Books, 2019.

DELL Technologies. **Sistema de arquivos distribuídos**. 2023. Disponível em: https://www.dell.com/pt-br/dt/learn/data-storage/distributed-file-system.htm. Acesso em: 20 mar. 2023.

DE SOUZA, Marcos; ALMEIDA, Fernanda Gomes; SOUZA, Renato Rocha. O termo Big Data: quebra de paradigma dos n-V's. In: **Workshop de Informação, Dados e Tecnologia-WIDAT**. Universidade Federal de Minas Gerais, 2018.

DO NASCIMENTO, Paulo Vitor Braga; DE ARAÚJO, Gustavo Medeiros. Requirement of telematic data in Brazilian criminal investigation: Diagnosis, process flow and chain of custody supported by blockchain technology. **Advanced Notes in Information Science**, v. 4, 2023.

FRIZZO-BARKER, Julie *et al*. *Blockchain* as a disruptive technology for business: A systematic review. **International Journal of Information Management**, v. 51, p. 102029, 2020.

GIL, Antonio Carlos *et al*. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

GODA, Kazuo; KITSUREGAWA, Masaru. The history of storage systems. **Proceedings of the IEEE**, v. 100, n. Special Centennial Issue, p. 1433-1440, 2012.

GOPALAN, S. Harihara *et al*. Digital forensics using *Blockchain*. **International Journal of Recent Technology and Engineering**, v. 8, n. 2, p. 182-184, 2019.

GUPTA, Manav. ***Blockchain*** **For Dummies - 2nd IBM Limited Edition**. John Wiley & Sons, Inc., 2018.

HILEMAN, Garrick; RAUCHS, Michel. 2017 global blockchain benchmarking study. **Available at SSRN 3040224**, 2017.

IBM *Blockchain.* **O que é a tecnologia *Blockchain?*** 2022. Disponível em: <https://www.ibm.com/br-pt/topics/what-is-*Blockchain* >. Acesso em: 10 dez. 2022.

JORGE, Higor Vinicius Nogueira *et al*. **Tratado De Investigação Criminal Tecnológica**. (n.p.): Juspodivm, 2021.

KHAN, Abdullah Ayub et al. MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. **IEEE Access**, v. 9, p. 103637-103650, 2021.

KUBE, Nicolas Daniel Drescher: ***Blockchain*** **basics: a non-technical introduction in 25 steps**: Apress, 2017, 255 p. ISBN: 978-1-4842-2603-2. 2018.

LI, Meng *et al*. LEChain: A *Blockchain* -based lawful evidence management scheme for digital forensics. **Future Generation Computer Systems**, v. 115, p. 406-420, 2021.

LONE, Auqib Hamid; MIR, Roohie Naaz. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. **Digital investigation**, v. 28, p. 44-55, 2019.

MANYIKA, *et al*. Big Data: The next frontier for innovation, competition, and productivity. **McKinsey Global Institute**, New York, 2011.

MARTINS, Leon Emerich Lentz; VIANNA, William Barbosa. Cap. 4: Proposta de elementos conceituais para investigação criminal sob influência da Ciência da Informação. **Aproximação entre a ciência da informação com a ciência policial**, SENAC, 2019.

MILAGRE, José Antônio; SEGUNDO, José Eduardo Santarém. As contribuições da Ciência da Informação na perícia em informática no desafio envolvendo a análise de grandes volumes de dados – Big Data. **Informação & Tecnologia (ITEC)**, Marília/João Pessoa, v. 2(2), n. 35-48, jul./dez 2015.

MILES, Matthew B.; HUBERMAN, A. Michael. **Qualitative data analysis: An expanded sourcebook**. Sage, 1994.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, p. 21260, 2008.

NEIVA, Laura. **Big Data na investigação criminal**: desafios e expectativas na União Europeia. Edições Húmus, 2020.

NGUYEN, Quoc Khanh; DANG, Quang Vang. *Blockchain* Technology for the Advancement of the Future. In: **2018 4th international conference on green technology and sustainable development (GTSD)**. IEEE, 2018. p. 483-486.

OECD/Eurostat. **Oslo Manual 2018**: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition, The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris/Eurostat, Luxembourg. 2018, p. 246. Disponível em: https://doi.org/10.1787/9789264304604-en.

ØLNES, Svein; JANSEN, Arild. Blockchain technology as infrastructure in public sector: an analytical framework. In: **Proceedings of the 19th annual international conference on digital government research: governance in the data age**. 2018. p. 1-10.

OLUKOYA, Oluwafemi. Distilling blockchain requirements for digital investigation platforms. **Journal of Information Security and Applications**, v. 62, p. 102969, 2021.

PAJEÚ, Hélio Márcio; MOURA, Rhayza Rodrigues; DE CARVALHO, David Oliveira. Organização e classificação para documentos digitais de arquivos pessoais nas nuvens. **[TESTE] Ciência da Informação em Revista**, v. 5, n. 3, p. 58-70, 2018.

PASTRANA-PARDO, Manuel-Alejandro; ORDÓÑEZ-ERAZO, Hugo-Armando; COBOS-LOZADA, Carlos-Alberto. Process Model Represented in BPMN for Guiding the Implementation of Software Development Practices in Very Small Companies Harmonizing DEVOPS and SCRUM. **Revista Facultad de Ingeniería**, v. 31, n. 62, 2022.

PATTON, Jeff; ECONOMY, Peter. **User story mapping: discover the whole story, build the right product**. O'Reilly Media Inc., 2014.

PETRONI, Benedito Cristiano Aparecido et al. Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain. **Forensic Science International: Digital Investigation**, v. 34, p. 300985, 2020.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos**. São Paulo: Marcial Pons, 2014.

RAJAMÄKI, Jyri; KNUUTTILA, Juha. Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-of-custody requirement. In: **2013 European Intelligence and Security Informatics Conference**. IEEE, 2013. p. 198-203.

RICHARDS, Mark. **Software architecture patterns**. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Incorporated, 2015.

SAISSE, Renan. Big Data Contra o Crime. **Revista Eletrônica Direito & TI**, v. 1, n. 8, p. 16, 2017.

SANTOS, Cleórbete.; PRATA, David Nadler Prata; ARAUJO, Humberto Xavier. **Fundamentos da Tecnologia *Blockchain.*** 1. ed. Amazon, 2019.

SARACEVIC, T.; EMPTY, Ciência da informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, v. 1, n. 1, p44, 1996. Disponível em: http://hdl.handle.net/20.500.11959/brapci/37415. Acesso em: 20 abr. 2022.

SARACEVIC, Tefko. Interdisciplinary nature of information science. **Ciência da informação**, v. 24, n. 1, p. 36-41, 1995.

SHRIMALI, Bela; PATEL, Hiren B. *Blockchain* state-of-the-art: architecture, use cases, consensus, challenges and opportunities. **Journal of King Saud University-Computer and Information Sciences**, v. 34, n. 9, p. 6793-6807, 2022.

SOUSA, Renato Tarciso Barbosa de. Classificação como função matricial do que fazer arquivística. 2007.

SWARAJ, Ananya. Exploratory Research: Purpose and Process. **Parisheelan Journal**, 2019.

TAPSCOTT, Don; TAPSCOTT, Alex. ***Blockchain* revolution**. Senai-SP Editora, 2018.

TELEMÁTICA. *In*: MICHAELIS, Dicionário Online de Português. Uol, 2023. Disponível em: < https://michaelis.uol.com.br/ >. Acesso em: 13 mar. 2023.

TIAN, Zhihong *et al*. Block-DEF: A secure digital evidence framework using *Blockchain*. **Information Sciences**, v. 491, p. 151-165, 2019.

WALPORT, Mark (Ed.). **Distributed ledger technology: Beyond block chain**. UNITED KINGDOM GOVERNMENT – Government Office for Science, 2016. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>. Acesso em: 13 mar. 2023.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. LVM Editora, 2017.

ZANINI, Walter. A arte de comunicação telemática: a interatividade no ciberespaço. **ARS (São Paulo)**, v. 1, p. 11-34, 2003.

APÊNDICE A – HISTÓRIAS DE USUÁRIO

Sumário

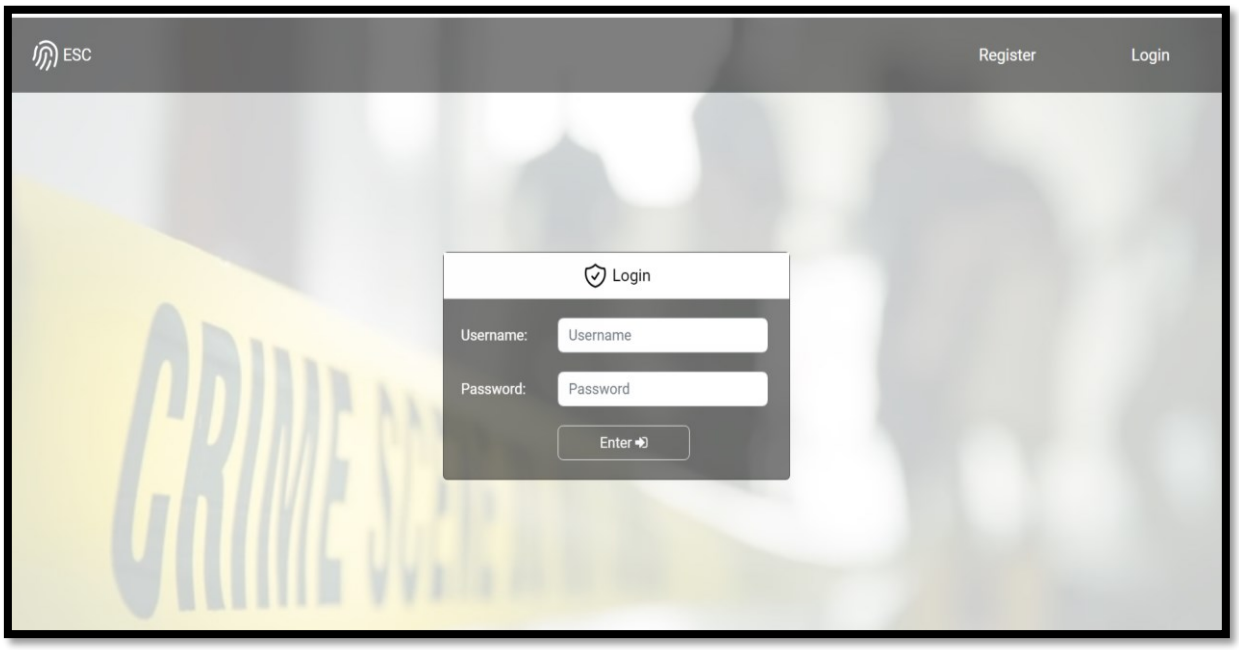
1 INTRODUÇÃO

A proposta deste documento é listar os requisitos funcionais mínimos, informando se existe dependência com outro requisito, realizando rastreabilidade das mensagens e regras de negócio, apresentando a forma de acesso e uma breve descrição das telas.

Seguindo os princípios do MVP (*Minimum Viable Product*), o produto viável mínimo, o documento aponta para uma versão mais simples com uma quantidade mínima de esforço e desenvolvimento que permita seu funcionamento. A versão demonstrativa do *layout* das telas do sistema permite uma melhor visualização dos requisitos e regras necessárias.

As telas e dados apresentados a seguir são fictícios e têm a finalidade exclusiva de ilustração. Nenhuma das informações exibidas reflete dados reais ou corresponde a uma situação concreta. O uso dessas telas é destinado apenas para demonstrar o funcionamento do sistema proposto.

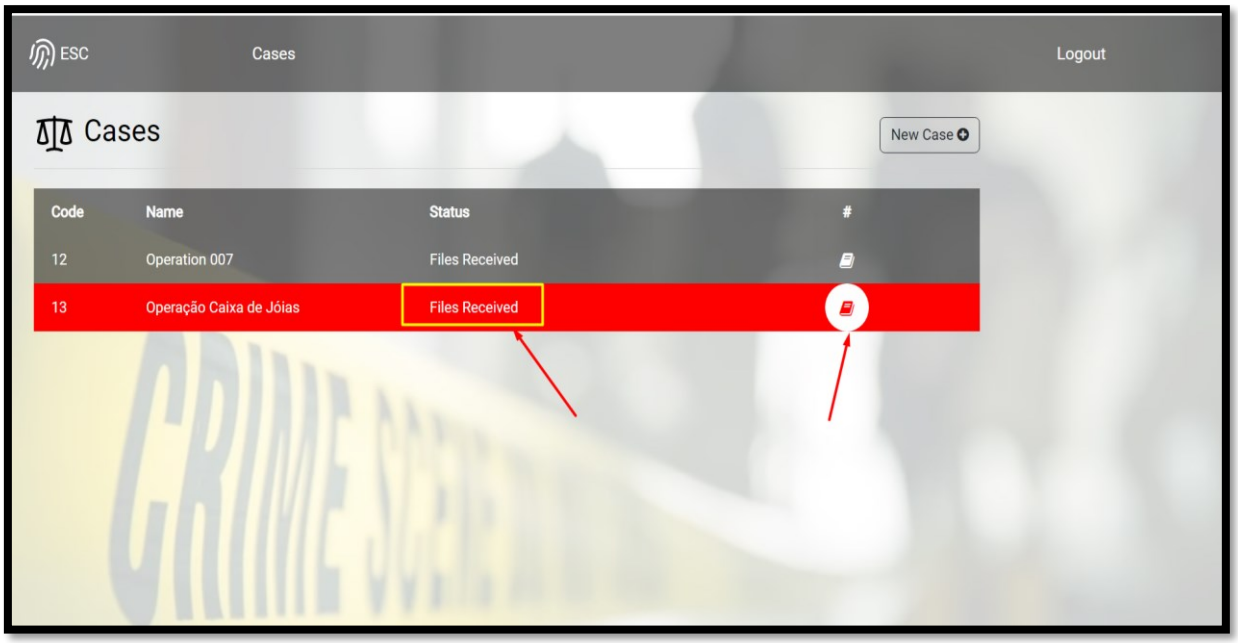
2 LOGIN

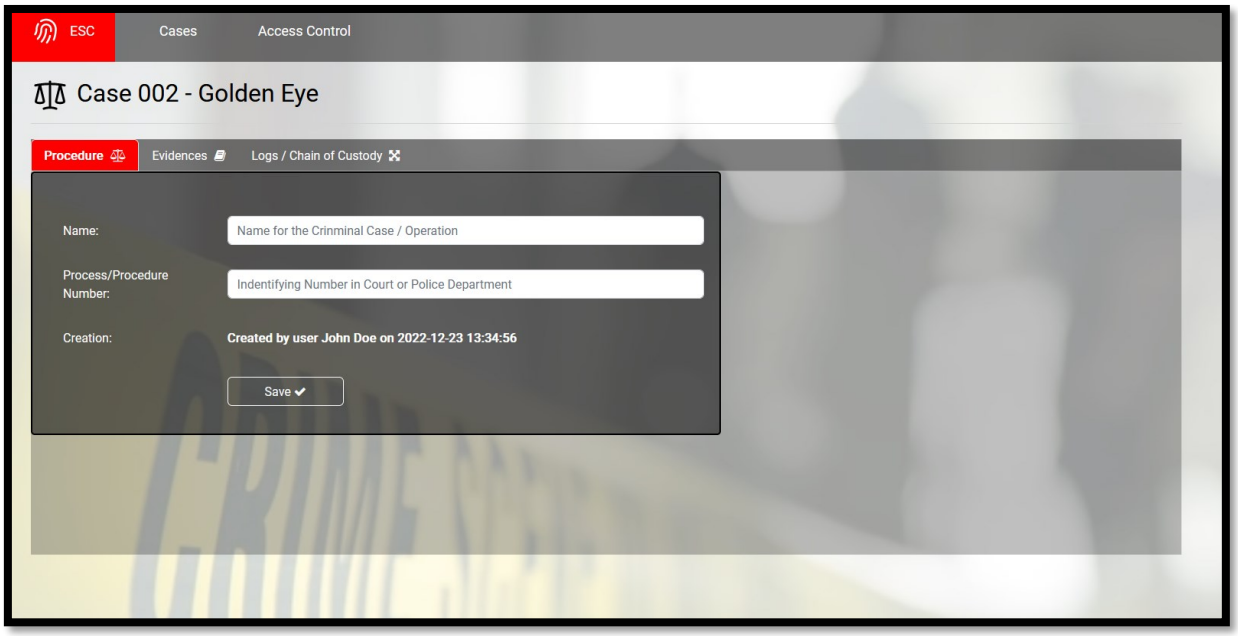


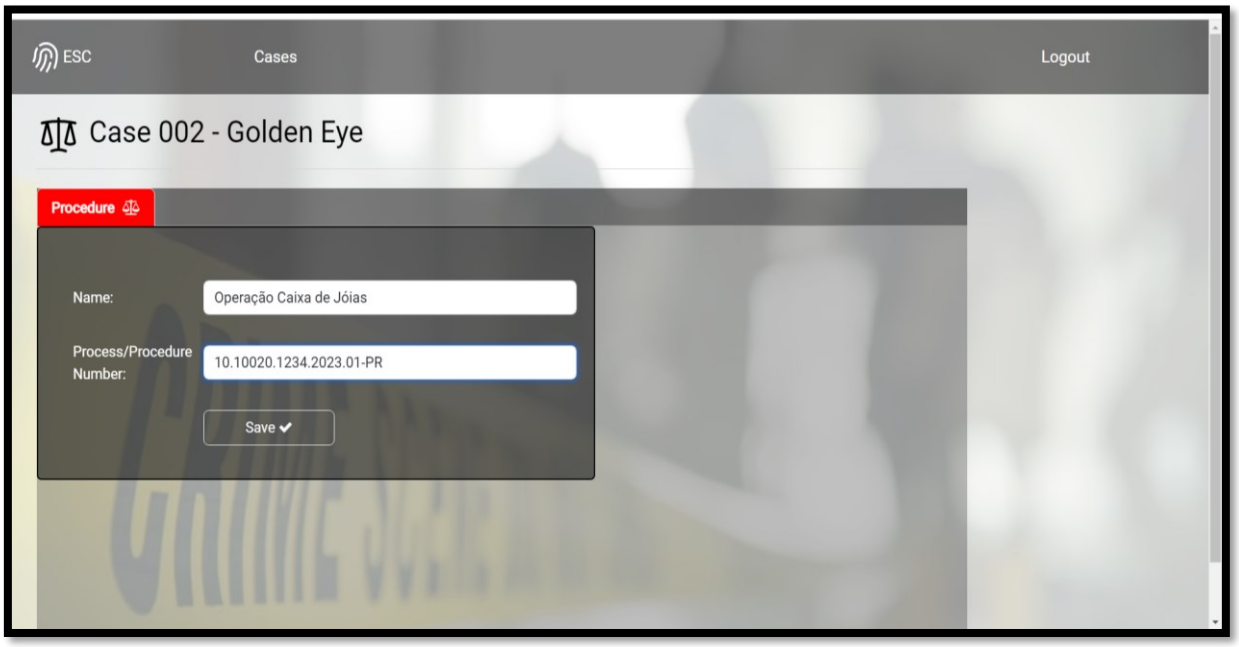
2.1 Login - Descrição da Tela protótipo

Nome do Campo	Descrição / Observação	Regras de Negócio
Login do usuário	• Campo de login e senha • Usuário entra com suas credenciais para logar no sistema.	Identificação do usuário que promoveu a ação; (usuário e órgão vinculado, empresa provedora, órgão e OI vinculado na ação realizada); Data/Hora da ação; Nome do usuário que promoveu a ação; Tipo de ação; Informação Auditada; (incluindo a justificativa, quando houver) CPF do Usuário logado; Código do Sistema (Código Interno do Sistema); IP do usuário que realizou a ação;
Registro do usuário	• Campo Registro	Registro do usuário que requer acesso ao sistema; (usuário e órgão vinculado, empresa provedora, órgão e OI vinculado na ação realizada); Dados pessoais e do órgão vinculado; CPF do Usuário; Código do Sistema (Código Interno do Sistema);

3 CASOS


ESC
Cases
Logout
Cases
New Case
Code
Name
Status
#
12
Operation 007
Files Received
13
Operação Caixa de Jóias
Files Received


ESC
Cases
Access Control
Case 002 - Golden Eye
Procedure
Evidences
Logs / Chain of Custody
Name:
Name for the Crinminal Case / Operation
Process/Procedure Number:
Indentifying Number in Court or Police Department
Creation:
Created by user John Doe on 2022-12-23 13:34:56
Save



3.1 Casos - Descrição da Tela protótipo

Nome do Campo	Descrição / Observação	Regras de Negócio
Aba novo caso	• Aba/Campo de criação de casos. • Usuário cria um caso.	Permite criar um caso novo e preencher os dados correspondentes.
Dados do caso	• Aba/Campo dados do procedimento • Usuário entra com informações do caso.	Identificação do procedimento judicial; Nome e número do processo, vara criminal correspondente e juiz do caso.
Dados do caso	• Aba/Campo dados do procedimento • Usuário visualiza o *status* do caso.	Permite visualização de todos os casos cadastrados; Permite visualização do status do caso; Arquivos recebidos, aguardando atendimento, download realizado, encerrado e correspondente provedor. Número de requisições solicitadas e correspondente provedor
Logout	• Campo/Botão para saída do sistema. • Usuário sai do sistema.	Permite sair do sistema de forma segura; Desconecta usuário do sistema.

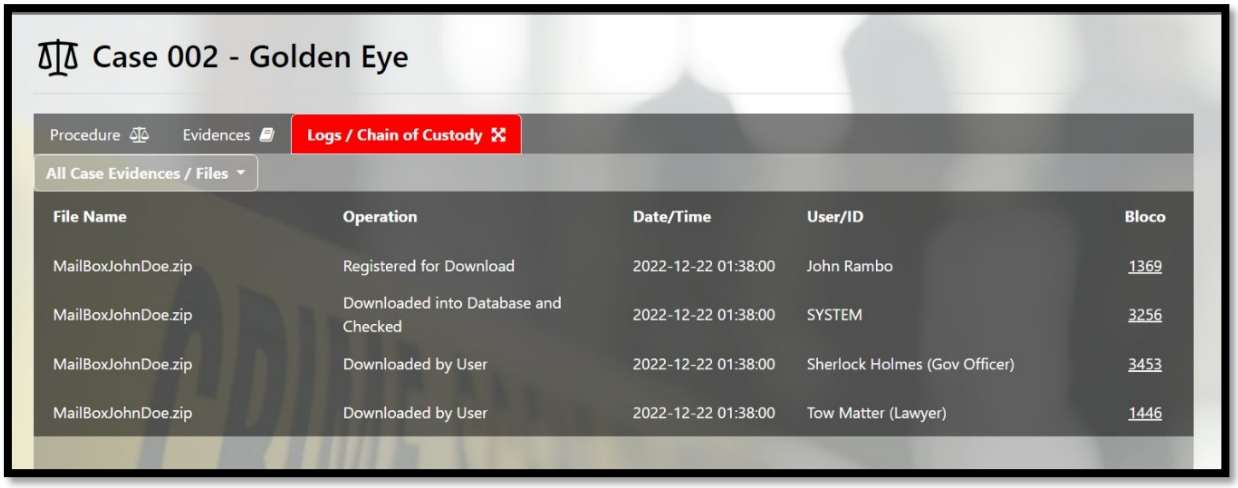
4 EVIDÊNCIA

4.1 Evidências - Descrição da Tela protótipo

Nome do Campo	Descrição / Observação	Regras de Negócio
Aba evidências	• Aba/Campo de evidências • Usuário visualiza as informações básicas e detalhadas (clicando) e status da evidência e pode realizar o download.	Permite visualizar dados básicos da evidência digital carregada; Nome do arquivo, tamanho, status, data do carregamento, data/hora do último download; Apresenta link para download do arquivo. Informações detalhadas ao clicar na evidência. Nome do caso, fonte de evidência (provedor), data/hora de fornecimento da evidência, data/hora da requisição da evidência, tempo de atendimento entre requisição e recebimento, usuário/grupo que realizou a operação. Nome do arquivo, Operação realizada (download/upload), data/hora da operação, identificação do usuário que realizou a operação, Bloco registrado na Blockchain, link do bloco para apresentado o explorador da Blockchain; Informações detalhadas ao clicar no provedor. Prazo médio de atendimento baseado nas datas de requisições e recebimentos. Volume total (tamanho) de arquivos recebidos pelo provedor. Percentual de

		requisições solicitadas comparados a outros provedores.
Logout	• Campo/Botão para saída do sistema. • Usuário sai do sistema.	Permite sair do sistema de forma segura; Desconecta usuário do sistema.

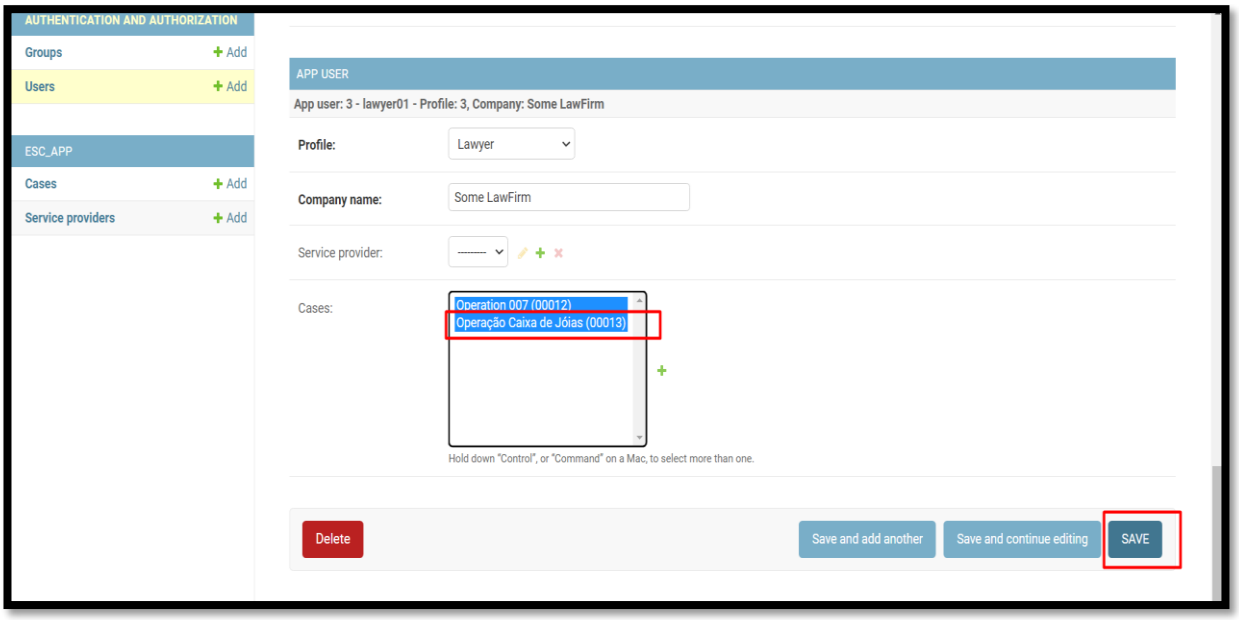
5 LOGS E CADEIA DE CUSTÓDIA



5.1 Logs e cadeia de custódia - Descrição da Tela protótipo

Nome do Campo	Descrição / Observação	Regras de Negócio
Aba logs/cadeia de custódia	• Aba/Campo logs/cadeia de custódia. • Usuário visualiza as informações básicas e detalhadas (clicando) da evidência.	Permite visualizar dados básicos da cadeia de custódia da evidência digital carregada; Nome do arquivo, Operação realizada (download/upload), data/hora da operação, identificação do usuário que realizou a operação, Bloco registrado na Blockchain, link do bloco para apresentado o explorador da Blockchain; Permite visualizar dados detalhados (clicando) da cadeia de custódia da evidência digital selecionada; Nome do caso, fonte de evidência (provedor), data/hora de fornecimento da evidência, data/hora da requisição da evidência, tempo de atendimento entre requisição e recebimento, usuário/grupo que realizou a operação. Nome do arquivo, Operação realizada (download/upload), data/hora da operação, identificação do usuário que realizou a operação, Bloco registrado na Blockchain, link do bloco para apresentado o explorador da Blockchain;

6 GESTÃO DE USUÁRIOS



6.1 Gestão de usuários - Descrição da Tela protótipo

Nome do Campo	Descrição / Observação	Regras de Negócio
Autenticação/Autorização – Grupos	• Aba/Campo Grupos • Usuário administrador cadastra/gerencia/configura os grupos e suas permissões que os usuários vinculados terão acesso.	Registro dos grupos de usuários que acessam o sistema; (Administradores, Usuários comuns/avançados, Judiciário, Ministério Público, Polícia, Defesa, Provedor de tecnologia); Dados e descrição das permissões do grupo vinculado; Código do Sistema (Código Interno do Sistema);
Autenticação/Autorização – Usuários	• Aba/Campo Usuários • Usuário administrador cadastra/gerencia/configura os usuários e suas permissões e que grupos aos quais pertencem.	Registro do usuário que requer acesso ao sistema; hierarquizado por permissões usuário comum, avançado e administrador, incluindo descrições das permissões de cada um (usuário/grupo e órgão vinculado, empresa provedora, órgão e OI vinculado na ação realizada); Dados pessoais e do órgão vinculado; CPF do Usuário; Código do Sistema (Código Interno do Sistema);
ESC APP – Casos	• Aba/Campo Casos • Usuário administrador cadastra/gerencia/configura os casos e suas informações relacionadas.	Permite criação e visualização de todos os casos cadastrados; Permite gestão/edição e visualização dos casos existentes e todas as suas informações;
ESC APP – Provedores de serviço	• Aba/Campo Provedores de serviço	Permite criação e visualização de todos os provedores de tecnologia. Descrição

	• Usuário administrador Cadastra/gerencia/configura os Provedores de serviço e suas informações relacionadas.	de permissões de acesso ao sistema; grupo vinculado, dados da empresa provedora, endereço e formas de contato; Relatórios de prazo médio de atendimento baseado nas datas de requisições e recebimentos. Volume total (tamanho) de arquivos recebidos pelo provedor. Percentual de requisições solicitadas comparados a outros provedores. Número de requisições solicitadas e correspondente provedor