DIRETORIA TECNICO-CIENTIFICA/DPF

Estudo Técnico Preliminar 70/2025

1. Informações Básicas

Número do processo: 08201.000148/2025-56

2. Descrição da necessidade

2.1. Motivação/Justificativa

2.1.1. No contexto das operações conduzidas pela Polícia Federal, bem como durante as ocorrências de flagrante, é recorrente a apreensão de aparelhos celulares e computadores, os quais são posteriormente submetidos a exames periciais para as respectivas extrações e análises de dados relevantes às investigações criminais. Esses dispositivos frequentemente contêm informações essenciais para a elucidação de crimes, como registros de comunicações, arquivos de mídia (imagens, áudios e vídeos, dentre outros), geolocalização e outros vestígios digitais de interesse probatório.

2.1.2. Diante desse cenário, as Unidades de Criminalística enfrentam o desafio de conduzir os exames periciais de maneira eficiente, garantindo que a extração e análise dos dados ocorram com a máxima celeridade, sem comprometer a integridade das informações e respeitando a cadeia de custódia. A necessidade de rapidez se justifica não apenas pela exigência de prazos processuais, mas também pela urgência de determinadas investigações, como aquelas relacionadas a organizações criminosas, crimes cibernéticos e delitos que demandam ação imediata das autoridades. Além disso, o avanço tecnológico constante exige atualizações contínuas dos métodos periciais para lidar com novas formas de segurança e criptografia presentes nos dispositivos móveis.

2.1.3. A perícia da Polícia Federal dispõe de um conjunto limitado de soluções tecnológicas para realizar a extrações, decodificações e análises de dados em seus laboratórios de informática forense. Essas ferramentas especializadas permitem a obtenção de evidências digitais armazenadas em dispositivos móveis, mídias e outros equipamentos eletrônicos, desempenhando um papel crucial na investigação criminal. Devido à diversidade de fabricantes, modelos e versões de dispositivos e sistemas operacionais, bem como aos constantes avanços na segurança e criptografia dos dispositivos, é comum que uma única ferramenta não seja suficiente para realizar a extração ou decodificação completa dos dados de um aparelho específico.

2.1.4. Pontua-se que a Polícia Federal investe no desenvolvimento de projetos internos altamente especializados, como o LED (Localizador de Evidências Digitais) e o IPED (Indexador e Processador de Evidências Digitais), ampliando sua capacidade de análise de evidências digitais. Porém, as soluções desenvolvidas internamente são especializadas para determinados tipos de tarefas, não sendo capazes de atender a todos os casos ou mesmo interpretar toda a variedade de dados encontrados nos dispositivos eletrônicos apreendidos. Diante desse cenário, é necessária a utilização de múltiplas ferramentas, garantindo que, quando uma delas não for capaz de acessar e interpretar certos dados, outras soluções possam ser empregadas para complementar essas análises periciais. Para isso, a Polícia Federal precisa utilizar um ecossistema diversificado de ferramentas forenses, que inclui soluções renomadas no mercado, como o conjunto de ferramentas da Cellebrite e o Magnet Graykey, usados para quebras de senhas e extrações de dados de celulares, Atola TaskForce e Tableau TX1 para duplicações periciais (espelhamentos) de mídias como HDs e pen drives, e o Magnet Axiom, usado para decodificação e interpretação de dados de computadores e celulares.

2.1.5. Nesse sentido, as boas práticas forenses indicam que é fundamental dispor de mais de uma ferramenta distinta para lidar com o mesmo problema, garantindo a redundância necessária para validar os resultados obtidos e aumentar as chances de sucesso na recuperação de informações críticas. Esse princípio fortalece a confiabilidade dos exames periciais, reduzindo as limitações das soluções forenses e garantindo a robustez das provas digitais apresentadas no curso das investigações. Dessa forma, a utilização combinada de diferentes soluções assegura que a perícia da Polícia Federal mantenha um alto nível de precisão e eficiência na análise de dispositivos eletrônicos, alinhando-se às melhores práticas internacionais na área de computação forense.

2.1.6. Neste sentido, esse processo visa a contratação de ferramenta pericial para análise de vestígios digitais relacionados a computadores (discos rígidos) e aparelhos celulares para manter e atualizar o parque tecnológico no que se refere às análises periciais desses dispositivos e mídias.

2.2. Alinhamento Estratégico

2.2.1. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

I) ID PCA no PNCP: 00394494000136-0-000016/2025

II) Data de publicação no PNCP: 14/05/2024

III) Id do item no PCA: 299

IV) Classe/Grupo: 182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA

V) Identificador da Futura Contratação: 200406-316/2025

2.2.2. O objeto da contratação também está alinhado com Planejamento Estratégico da Polícia Federal 2024-2027 e com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) *2024-2027* da Polícia Federal, conforme demonstrado abaixo:

2.2.2.1. Planejamento Estratégico da Polícia Federal 2024-2027

Enfrentar a Criminalidade com Eficiência: KR5: Diminuir em 10% o tempo médio de atendimento das requisições periciais (DITEC)

2.2.2.2. Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC PF 2024-2027:

Objetivo Estratégico	ID da Necessidade	Necessidade de TIC	ID da Ação	Ação
4- Formar a polícia do futuro, moderna e inovadora	N7	Manutenção, aquisição, evolução e desenvolvimento de soluções de TIC	A155	Contratar hardware, licenças e softwares para exames periciais

3. Área requisitante

Área Requisitante	Responsável
SERVIÇO DE PERÍCIAS EM INFORMÁTICA - SEPINF/DPDCE/INC /DITEC/PF	LUIS FILIPE DA CRUZ NASSIF

4. Necessidades de Negócio

ID	REQUISITO
RN1	Decodificação e interpretação de dados de computadores e celulares;
RN2	Suporte para múltiplos dispositivos em uma mesma visão, com o objetivo de realizar uma análise integrada entre as evidências apreendidas.
RN3	Suporte aos sistemas operacionais Windows, macOS e Linux
RN4	Suporte aos sistemas operacionais iOS e Android;
RN5	Decodificação e análise de dados provenientes de nuvem;
RN6	Suporte a ferramentas que auxiliem na análise de casos envolvendo abuso sexual infantil
RN7	Direito de atualização e suporte técnico por 36 meses.
RN8	Suporte técnico (8X5).
RN9	Compatibilidade com a Arquitetura Tecnológica dos laboratórios forenses da Polícia Federal.

5. Necessidades Tecnológicas

ID	Descrição
RT1	Possuir suporte à decodificação de dados de dispositivos móveis, HDD, SSD, dispositivos USB e pastas de arquivos
RT2	Permitir a decodificação de dados de sistemas operacionais Windows, macOS, Linux
RT3	Permitir a decodificação de dados de dispositivos móveis com sistemas operacionais Android e iOS

RT4	Gerar relatórios nos formatos XML, HTML, CSV ou XLS, PDF e em formato portátil
RT5	Permitir o cálculo de HASH MD5 e SHA-256
RT6	Permitir realizar pesquisas utilizando textos, keyword, REGEX e GREP
RT7	Permitir realizar a decodificação e análise dos dados utilizando uma única plataforma
RT8	Permitir aplicação de filtros para auxiliar a pesquisa por artefatos
RT9	Permitir realizar a marcação de arquivos por meio de tags
RT10	Permitir gerar visualização utilizando Timeline
RT11	Permitir visualizar dados que possuem dados geográficos no mapa (geolocalização)
RT12	Permitir realizar uma pré-visualização dos arquivos analisados em uma mesma interface
RT13	Permitir visualizar os arquivos no formato Hexadecimal para uma análise mais detalhada dos dados
RT14	Permitir a exportação dos dados encontrados no arquivo de evidência
RT15	Permitir a recuperação de arquivos deletados e não sobrescritos
RT16	Permitir colaboração e compartilhamento de evidências
RT17	Permitir recuperar o Backups do iTunes
RT18	Permitir recuperar informações quando um arquivo de torrent foi criado, modificado e baixado
RT19	Permitir busca por palavra-chave em sistema de arquivos
RT20	Permitir analisar artefatos P2P em dispositivos Android
RT21	Permitir verificação baseada em Hash de imagem forense E01
RT22	Possuir interface em no mínimo Inglês ou Português – Brasileiro
RT23	Permitir a inserção da chave de criptografia de um disco criptografado com BitLocker antes do processamento do mesmo

RT24	Permitir a criação de perfis de artefatos para diferentes tipos de casos
RT25	Possuir a capacidade de realizar o correlacionamento dos dados
RT26	Possuir funcionalidade de Inteligência Artificial para auxiliar na identificação de evidências, com suporte para interações em linguagem natural através de assistente virtual (chat).
RT27	Suporte a Imagens forenses de evidências no mínimo com os seguintes formatos de arquivo: E01, Ex01, L01, Lx01, AD1, dd, raw, bin, img, dmg, vmdk, vhd, vdi, xva, ufd, ufdx, zip, tar;
RT28	Suporte para decodificação e análise de dados extraídos com as ferramentas forenses Cellebrite Inseyts e Magnet GrayKey
RT29	Suporte aos sistemas de arquivos: NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2, APFS
RT30	Detecção automática de criptografia Truecrypt, Bitlocker, PGP, e Safeboot
RT31	Capacidade de pré-visualização de arquivos plist
RT32	Capacidade de pesquisa do espaço não alocado em uma imagem APFS
RT33	Suporte de análise para itens recuperados de $RECYCLE.BIN
RT34	Permitir a decodificação e análise da dados capturados de memória RAM
RT35	Permitir a comparação de hashes com bases especializadas, como Project VIC
RT36	Capacidade de análise de retorno de mandados judiciais de dados provenientes de nuvens, considerando ao menos Instagram, Facebook, Snapchat, Twitter, Google e Apple.
RT37	Uso de tokens extraídos da memória de aparelho celular para acesso a serviços e cópia forense de dados de serviços com armazenamento de dados na nuvem, contornando o segundo fator de autenticação, se necessário.
RT38	Localização e extração de tokens do computador (Windows, macOS)
RT39	Reconstrução de páginas WEB
RT40	Recuperação de dados públicos de redes sociais

RT41	Suporte fontes com duplo fator de autenticação
RT42	Permitir agregar várias fontes de dados em um único caso
RT43	Permiti detectar automaticamente possíveis imagens de conteúdo ilícito, como abuso infantil, substâncias proscritas e armas.
RT44	Permitir a identificação de carteiras, chaves privadas e análise de transações em blockchain, auxiliando em investigações envolvendo criptomoedas
RT45	Visualização de SQLite
RT46	Visualização em formato Hexadecimal
RT47	Visualização de geolocalização em mapas
RT48	Definir e alterar fuso horário padrão
RT49	Customização de relatórios
RT50	Recuperação de imagens, localizações, strings e demais arquivos apagados (carving)
RT51	Tratamento de banco de dados de aplicativos não categorizados, através do banco de dados (Assistente do SQLite)
RT52	Geração de dicionário de palavras e números, para ser utilizado como referência de ataque para quebra de senha
RT53	Customização e execução de scripts Python
RT54	Permitir atualização e suporte técnico por 36 meses
RT55	Fornecer Suporte técnico (8X5)
RT56	Compatibilidade com a arquitetura tecnológica dos laboratórios forenses de informática, com Workstations baseadas prioritariamente em Sistemas Operacionais Windows

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

6.1.1. Deverão ser adotadas pela CONTRATADA as normas federais, estaduais e distritais quanto aos critérios de preservação ambiental.

6.1.2. A empresa CONTRATADA deverá declarar ter conhecimento da Política de Sustentabilidade, observar, no que couber, as diretrizes de sustentabilidade ambiental, dando cumprimento aos dispositivos contidos na Instrução Normativa SLTI/MPOG nº 01, de 19/01/2010 e na 7ª edição do Guia Nacional de Contratações Sustentáveis da Advocacia Geral da União - outubro de 2024.

6.1.3. Os profissionais da CONTRATADA, com vistas a redução de impactos negativos sobre o meio ambiente, deverão estar informados sobre as boas práticas adotadas pela Polícia Federal voltadas ao consumo consciente, redução de desperdício e coleta seletiva, com objetivo de contribuir para a preservação do meio ambiente e dos recursos públicos.

6.1.4. A contratada se responsabilizará pela adequada destinação de equipamentos e demais acessórios essenciais à prestação dos serviços e adotará critérios compatíveis com padrões de consumo sustentáveis.

6.2. A demanda do órgão tem como base as seguintes características:

6.2.1. A licença deverá atender 50 (cinquenta) Unidades de Criminalísticas, conectadas à rede com domínio da Polícia Federal;

6.2.1. A CONTRATANTE terá o direito de utilizar o software objeto deste contrato em qualquer região do território nacional, sem necessidade de prévia comunicação ou autorização da CONTRATADA. Não haverá restrição de uso relacionada à localização física de dongles, endereços IP, geolocalização, acesso remoto, como por exemplo via redes virtuais privadas (VPN), ou infraestrutura tecnológica utilizada pela CONTRATANTE.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Em sua estrutura atual (Decreto nº 11.759/2023 e Portaria MJSP nº 542/2023), a Polícia Federal se faz presente em 123 cidades brasileiras. Em termos da estrutura da Perícia, há 27 Setores Técnico-Científicos, que contam com o apoio de 22 Núcleos Técnico-Científicos localizados no interior do país, além do Instituto Nacional de Criminalística, localizado em Brasília, estando presente, portanto, em 49 cidades. Neste sentido, na estimativa da demanda é observado como **primeira premissa** a necessidade de abranger todas as Unidades de Criminalística.

7.2. Dados de fevereiro de 2025 indicam a quantidade de Peritos com formação específica na área de informática (Peritos Criminais Federais da área 3) que atuam na especialidade de extração e análise de dados de dispositivos computacionais (telefones celulares, tablets, computadores, entre outros), conforme observado na figura 1:

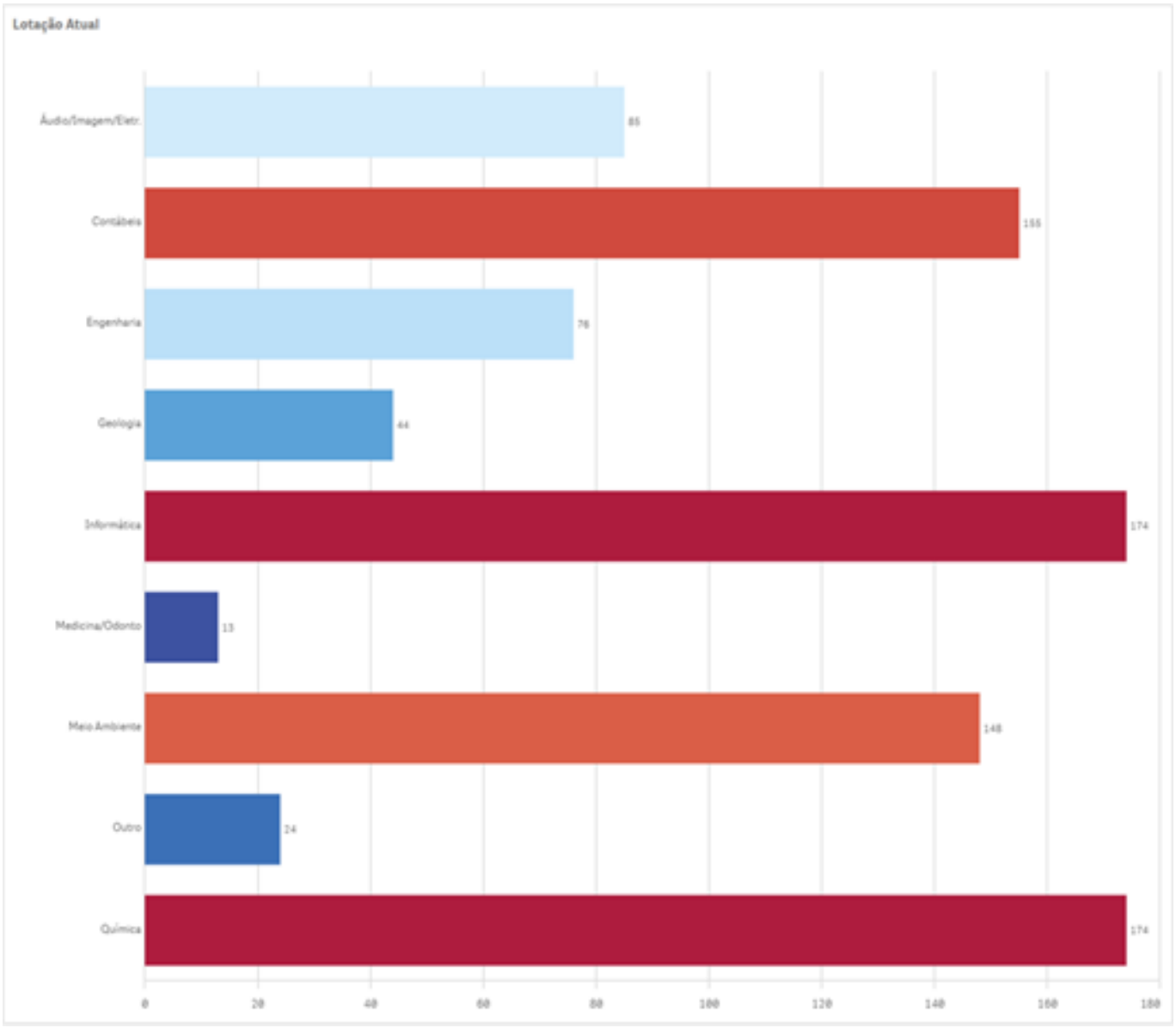

Figura 1 – Lotação atual dos Peritos Criminais Federais (fevereiro/2025).

7.3. Conforme observado, em fevereiro de 2025, o Sistema Nacional de Criminalística contava com 174 (cento e setenta e quatro) servidores especializados e desempenhando, mesmo que às vezes parcialmente, exames de extração e análise de dados de dispositivos computacionais e mídias.

7.4. Se for considerado uma disponibilidade média de atuação do perito, que leve em conta ausências por licenças e afastamentos, atuação em outras atividades prioritárias da unidade, participação em operações policiais, etc, a quantidade de Peritos disponíveis na área de informática cai para 100, conforme figura 2:

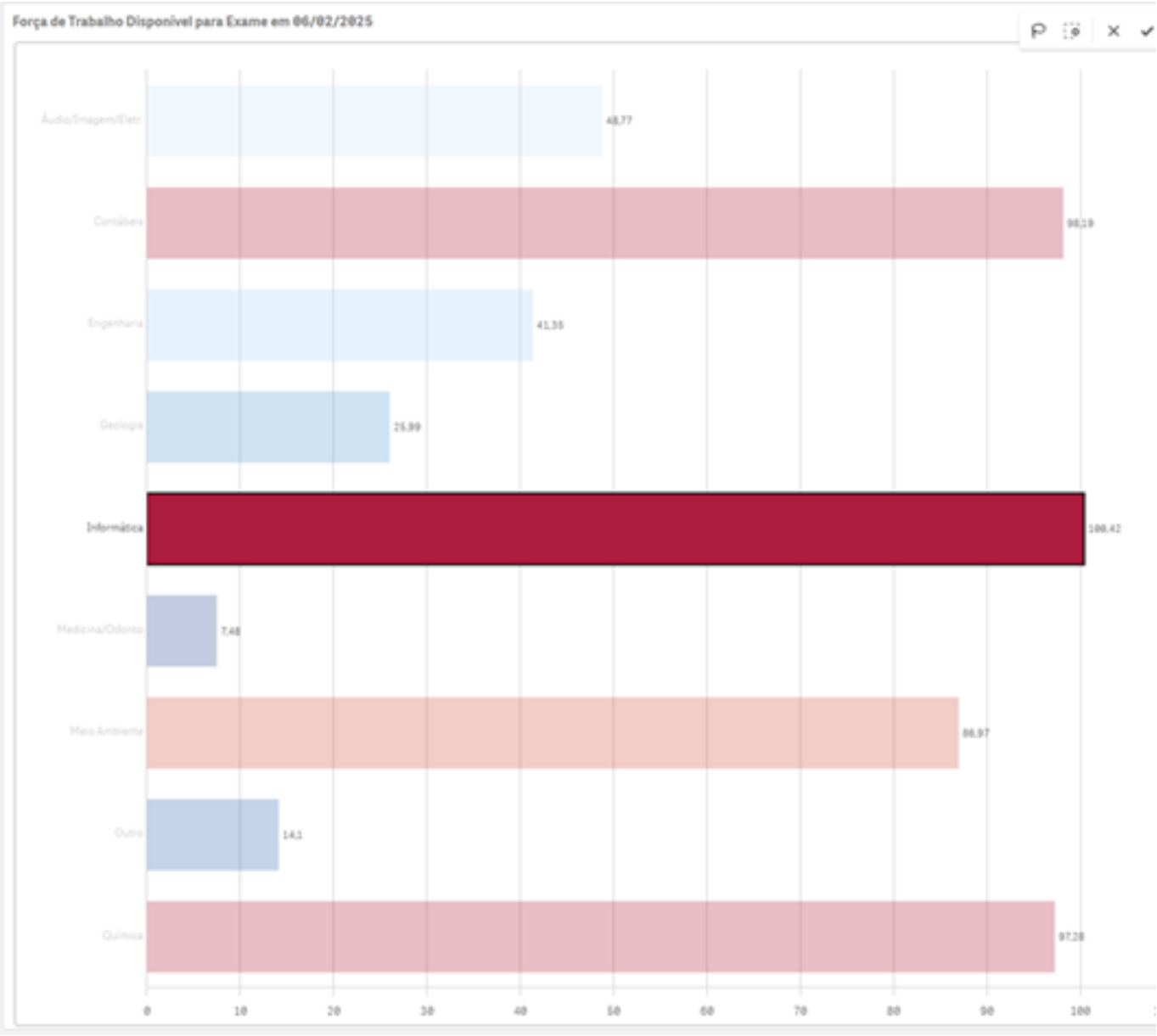

Figura 2 – Força de trabalho disponível para exames em fevereiro de 2025.

7.5. Em um cenário ideal, cada Perito que trabalha com essa especialidade deveria possuir as ferramentas adequadas à pronto uso. Isso seria de interesse para a investigação criminal, uma vez que não haveria gargalos na utilização de ferramentas, refletindo em um menor tempo de atendimento.

7.6. Em um segundo cenário, intermediário, cada Unidade de Criminalística deveria possuir ao menos uma ferramenta especializada para compartilhamento entre os peritos.

7.7. Todavia, há uma clara necessidade de otimização do uso dessas ferramentas, considerando o cenário de recursos orçamentários limitados.

7.8. Conforme mencionado na “Nota Técnica AudTI/TCU 8/2023 – Elaboração do orçamento estimado de contratações públicas de bens e serviços de TI” (página 462, item 916), nem sempre é possível se estimar quantidades baseado em premissas ou parâmetros de entrada irrefutáveis. Assim, na medida possível, “os gestores envolvidos devem tomar providências para diminuir ou eliminar essas limitações com o tempo.”. Neste sentido, adota-se como **segunda premissa** a necessidade de compartilhamento da ferramenta entre 50 (cinquenta) Unidades de Criminalística, para uso dos 174 servidores especializados.

7.9. Outro fator importante a ser levado em consideração, é o volume de serviço, que pode ser medido através da quantidade de requisições de laudos e da métrica adotada para valorar o esforço do exame, definido pela DITEC como “Objeto de Exame”.

7.10. De acordo com a Portaria nº 1.027/2021-DITEC/PF (SEI 143058902) que delimita o cadastramento de parâmetros para viabilizar a estimativa das complexidades dos exames periciais e conforme dados obtidos no BI da PF, houve um total de 14.791 registros de solicitações de exames periciais para a área de informática, que geraram um total de 45.734,10 pontos de complexidade da solicitação do exame (pontos de Objetos de Exames).

Ano de registro	2024		
Classe / Subclasse de Exame	Total de registros	Sum of Soma de pontuação de complexidade da solicitação de exame	
Laudo de Aplicação de Técnicas para Acesso a Dados - Sem Sucesso	242	362,93	0,85%
Laudo de Cópia Forense de Dados	142	201,55	0,47%
Laudo de Descrição de Material de Informática	11	3,32	0,01%
Laudo de Exame de Análise Comportamental	8	10,00	0,02%
Laudo de Exame de Análise de Conteúdo	1.861	16.827,47	39,32%
Abuso Sexual Infantojuvenil	1.148	12.146,59	28,38%
Outra	76	374,50	0,88%
(blank)	637	4.306,38	10,06%
Laudo de Exame de Análise de Funcionalidade	32	130,10	0,30%
Laudo de Exame de Ataque Cibernético	10	173,00	0,40%
Laudo de Exame de Constatação de Arquivos de Abuso Sexual Infantojuvenil	213	638,55	1,49%
Laudo de Exame de Dispositivo de Armazenamento Computacional	54	169,80	0,40%
Laudo de Exame de Equipamento Computacional	2	0,00	0,00%
Laudo de Exame de Equipamento Computacional Portátil	99	184,65	0,43%
Laudo de Exame de Extração Avançada de Dados (JTAG/ISP, chip-off)	17	52,45	0,12%
Laudo de Exame de Extração Forense de Dados	8.294	17.889,51	41,80%
Laudo de Exame de Extração Forense e Filtragem de Dados	2.097	4.685,92	10,95%
Laudo de Exame de Local da Internet	6	11,50	0,03%
Laudo de Exame de Local de Informática	36	206,25	0,48%
Laudo de Exame de Preservação de Conteúdo	102	183,20	0,43%
Laudo de Exame de Quebra Especializada de Senha	310	658,12	1,54%
Laudo de Exame de Quebra Especializada de Senha - Insucesso	118	94,64	0,22%
Laudo de Exame de Reparação Física	19	36,05	0,08%
Laudo de Exame de Sistema Informatizado	22	280,90	0,66%
(blank)	1.096	2.934,19	
Grand Total	14.791	45.734,10	

Figura 3 – Registros de exames e somatório da complexidade da solicitação. Exames na área de Informática realizados em 2024.

7.11. Conforme observado na figura 3, do total de pontuação de complexidade (Objetos de Exames), cerca de 40% foram de análise de conteúdo, que exigem uma maior aplicação de técnicas periciais e ferramentas especializadas. Para estes exames, são utilizadas ferramentas proprietárias, bem como a ferramenta IPED, desenvolvida por Peritos da PF. É razoável, portanto, definir que em 50% do tempo de análise é utilizado a ferramenta IPED e 50% uma ferramenta proprietária especializada, como o Magnet AXIOM.

7.12. A partir da análise dos dados, obtêm-se a **terceira premissa**, qual seja, a utilização de dados do histórico de produção e medidas de objetos de exames em trabalhos de análises de conteúdos da área de informática.

7.13. Memória de cálculo:

A) Premissas:

1. Necessidade de abranger todas as Unidades de Criminalística;

2. Necessidade de compartilhamento da ferramenta entre 50 (cinquenta) Unidades de Criminalística, para uso dos 174 servidores especializados;

3. Utilização de dados do histórico de produção e medidas de objetos de exames em trabalhos de análise de conteúdo da área de informática.

B) Fórmula de Cálculo.

1. Obter o total da força de trabalho pericial disponível para exames, considerando a área de informática.

2. Obter o percentual de exames realizados na Classe “Exame de Análise de Conteúdo”, em relação ao total de exames.

3. Obter o racional entre o total de força de trabalho disponível e o percentual de exames de análise de conteúdo.

4. Estimar a quantidade de licenças proprietárias necessárias, considerando a estimativa de que 50% do tempo será utilizada a ferramenta IPED e 50% a ferramenta proprietária.

C) Execução dos Cálculos:

Força de trabalho pericial disponível para exames, considerando a área de informática. (figura 2)	100
Percentual de exames realizados na Classe “Exame de Análise de Conteúdo”, em relação ao total de exames. (figura 3)	39,32%
Força de trabalho disponível X Percentual de exames de análise de conteúdo.	100 x 39,32% 40
Quantidade de licenças proprietárias necessárias, considerando a estimativa que 50% do tempo será utilizada a ferramenta IPED e 50% a ferramenta proprietária	40 x 0,5 = 20 licenças

7.14. As estatísticas apresentadas mostram que um Perito da área de informática dedica, em média, 40% do seu tempo para realizar análises de conteúdo. Tarefa essa que requer ferramentas especializadas. Neste cenário, buscando uma otimização do uso das ferramentas disponíveis, a fim de evitar eventuais períodos de baixa utilização, esse proporcional foi considerado para a estimativa das quantidades de licenças necessárias, chegando a um racional de cálculo de 20 (vinte) licenças.

7.15. Além disso, considerando que há 50 (cinquenta) unidades no Sistema de Criminalística da Polícia Federal e um total de 174 servidores especializados na área de informática (com disponibilidade média de 100 servidores), deverá ocorrer o compartilhamento das licenças entre os servidores, de acordo com as necessidades e a dinâmica das operações da PF.

8. Levantamento de soluções

8.1. A análise comparativa de soluções considera a possibilidade de aquisição na forma de bens ou contratação como serviço, fatores econômicos, aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, bem como as necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual, conforme art. 11, inciso II, da IN 94/2022 SGD/ME.

8.2. Para a elaboração da análise comparativa, serão observadas, caso existam, a possibilidade de ampliação ou substituição da solução já implantada no órgão, a disponibilidade de solução similar já adotada em outro órgão ou entidade da Administração Pública, as principais alternativas do mercado, os diferentes modelos de prestação do serviço, os distintos tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes.

8.3. Serão avaliadas, ainda, as políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, Infraestrutura de Chaves Públicas Brasileira - ICPBrasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis.

8.4. Considerando que se trata de contratação de licenças de softwares, serão observadas as soluções disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, que dispõe sobre a disponibilização de Software Público Brasileiro e dá outras providências.

8.5. Além disso, registra-se que foram observadas as diretrizes dispostas no Anexo I, item 1, da IN SGD/ME Nº 94 /2022 e a Portaria SGD/MGI nº 750, de 20 de março de 2023.

8.6. Dessa forma, segue abaixo o estudo das possíveis soluções:

Id	**Descrição da solução (ou cenário)**
1	Contratação de ferramenta pericial para análise de vestígios digitais relacionados a computadores (discos rígidos) e aparelhos celulares.
2	Utilização de softwares livres que possibilitem a análise de vestígios digitais relacionados a computadores (discos rígidos) e aparelhos celulares
3	Desenvolvimento interno de solução para análise de vestígios digitais relacionados a computadores (discos rígidos) e aparelhos celulares. (Desenvolvimento *in-house*).

9. Análise comparativa de soluções

9.1. ANÁLISE DAS SOLUÇÕES

9.1.1. Para a prospecção de soluções de mercado e softwares públicos, buscou-se junto ao SEPINF/DPDCE/INC /DITEC/PF o histórico de ferramentas forenses já utilizados pela Polícia Federal, bem como a identificação de outras ferramentas, ainda que não em uso pela PF.

9.1.2. Compete ao SEPINF as atribuições institucionais de aprimorar as metodologias relacionadas aos exames periciais em sua área de atuação, bem como propor medidas relacionadas à padronização desses laudos, conforme competências definidas pela IN 13/2005-DG/DPF, art.91, II e VII:

> (...) **Art. 91. Ao Serviço de Perícias em Informática compete:**
>
> (...) II - pesquisar, avaliar, desenvolver e aprimorar técnicas e metodologias relacionadas aos exames periciais correlatos à sua área de atuação;
>
> (...) VII - propor medidas relativas à padronização de laudos, ao controle de qualidade e a outros procedimentos relacionados às suas atividades específicas.

9.1.3. Neste contexto, observaram-se soluções já implementadas nos laboratórios das Unidades de Criminalística. Adicionalmente, foram analisadas soluções prospectadas e apresentadas em eventos de renome nacionais e internacionais. Entre estes eventos, destaca-se a Conferência Internacional de Ciências Forenses - INTERFORENSICS, realizada em agosto de 2025, bem como o Encontro Técnico de Perícias em Informática, que ocorreu em 2024 e reuniu no INC Peritos Criminais Federais da área de Informática.

9.1.4. Em complemento, foram realizadas buscas no Portal de Software Público (https://softwarepublico.gov.br /social/search /software_infos) e no Catálogo de Soluções de TIC com Condições Padronizadas, mantido pelo Órgão Central do SISP e disponível no sitio https://www.gov.br/governodigital/ptbr/contratacoes/catalogo-de-solucoes-de-tic.

9.1.5. Como já observado em outros processos de aquisição de ferramentas forenses, a descoberta das melhores soluções de análise forense no mercado não é trivial, pois há poucos materiais públicos acessíveis. Para identificação das soluções, além daquelas mapeadas internamente, foram pesquisados contratos firmados por órgãos que trabalham com a segurança pública, como o Ministério da Justiça, Ministério Público Federal e estaduais e polícias civis. Para isso, foram realizadas pesquisas nos sites Banco de Preços (www.bancodeprecos. gov.br) e painel de preços (https://paineldeprecos. planejamento.gov.br/) utilizando como termos as ferramentas analisadas com o intuito de identificar as soluções utilizadas em outros órgãos ou entidades da Administração Pública.

9.1.6. Considerando a experiência interna e a pesquisa definida no parágrafo anterior, foram definidos os maiores players do mercado forense que atendem total ou parcialmente os requisitos definidos neste estudo, listados a seguir.

Solução 1: Quanto às ferramentas comerciais, destaca-se:

9.1.7. Ferramenta Cellebrite UFED:

9.1.7.1. Cellebrite é uma empresa israelense que fabrica dispositivos de extração, transferência e análise de dados para telefones celulares e dispositivos móveis. Em 2007, a Cellebrite anunciou uma linha de produtos denominada 'Universal Forensic Extraction Device' (UFED), em português 'Dispositivo Universal de Extração Forense', destinada aos setores de forense e de investigação digital de aparelhos móveis.

9.1.7.2. O Cellebrite UFED é uma solução integrada que abarca desde o hardware, os softwares, os cabos e os acessórios necessários para o desbloqueio, extração e análise de dispositivos eletrônicos portáteis. Trata-se de uma solução voltada especificamente para análise de dispositivos portáteis. A sua interface integrada permite a realização de todas as fases necessárias para a análise desses equipamentos, desde o seu desbloqueio até a análise de dados específicos, tais como os provenientes de redes sociais, mensageria e serviços em nuvem.

9.1.7.3. Como ferramenta de decodificação e análise de dados, disponibiliza o software forense Cellebrite Physical Analyser.

9.1.8. Ferramenta Magnet AXIOM

9.1.8.1. A Magnet Forensics Inc., empresa sediada no Canadá e com escritório regional nos Estados Unidos. Atualmente, conta com um portfólio amplo de softwares para desempenhar atividades relacionadas a e-discovery. No contexto de análise de dados, destaca-se o software Magnet Axiom que, conforme descrição do produto no próprio site da empresa, é uma ferramenta para recuperação, análise e geração de relatório de dados de fontes como: computadores, celulares, nuvem e veículos.

9.1.8.2. A ferramenta Axiom não apresenta conjunto de cabos específicos ou hub para a realização de análise de dados. É uma ferramenta conhecida no mercado por sua capacidade de lidar com a análise de artefatos provenientes de internet e, nos últimos anos, tem investido fortemente na área computacional e de dispositivos celulares.

9.1.9. Ferramenta Oxygen Forensic Detective

9.1.9.1. O Oxygen Forensics é um conjunto de ferramentas forenses comerciais desenvolvidas pela Oxygen Forensics, Inc., projetado para a extração, análise e investigação de dados provenientes de dispositivos móveis, serviços em nuvem, computadores e drones. Ele se destaca pela sua capacidade de acessar e decodificar informações armazenadas em smartphones, tablets, wearables e aplicativos de comunicação, além de fornecer suporte para análise de dados extraídos de serviços como Google, iCloud, Facebook, WhatsApp e Telegram.

9.1.9.2. Com funcionalidades avançadas, o Oxygen Forensic Detective permite realizar extrações físicas, lógicas e baseadas em backups, além de descriptografar bancos de dados de aplicativos, recuperar mensagens apagadas e gerar relatórios detalhados. Ele também possui ferramentas para análise de redes Wi-Fi, localização geográfica, reconhecimento facial e detecção de manipulação em imagens.

9.1.10. MSAB Analyze - XAMN

9.1.10.1. O MSAB Analyze - XAMN é uma solução forense desenvolvida pela MSAB, especializada na análise e visualização de dados extraídos de dispositivos móveis. Ele é projetado para estruturar e interpretar informações obtidas por ferramentas de extração, como o MSAB Extract - XRY, e outras soluções forenses.

9.1.10.2. A ferramenta permite que investigadores realizem buscas avançadas, filtragem de dados e correlação de evidências entre múltiplos dispositivos, além de oferecer funcionalidades como análise de registros de chamadas, mensagens, histórico de localização e arquivos de mídia. O XAMN também apresenta visualizações detalhadas, incluindo linha do tempo interativa, mapas geoespaciais e diagramas de conexões, auxiliando na identificação de padrões e relacionamentos entre suspeitos.

9.1.11. Catálogo de Soluções de TIC com Condições Padronizadas definido pelo Órgão Central do SISP:

9.1.11.1. Destaca-se também que, o art. 2º, inciso XXVII, da IN SGD/ME nº 94/2022 define o Catálogo de Soluções de TIC com Condições Padronizadas como uma relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço, Preço Máximo de Compra de Item de TIC, entre outros.

9.1.11.2. Neste sentido, foi realizada a consulta ao Catálogo de Soluções de TIC com Condições Padronizadas, mantido pelo Órgão Central do SISP e disponível no sítio https://www.gov.br/governodigital/pt-br/contratacoes /catalogo-de-solucoes-de-tic, conforme documento SEI 143057834. Porém, nenhum software definido neste catálogo atende aos requisitos deste ETP.

Solução 2: Quanto às ferramentas de softwares livres (ou com código fechado, mas gratuito), destaca-se:

9.1.12. Não foram encontradas soluções de software no Portal de Software Público Brasileiro que atendam aos requisitos deste ETP. Foi utilizada a seguinte palavra-chave no campo de busca: Forense; Celular. Realizada em fevereiro/2025.

9.1.13. Fonte: https://softwarepublico.gov.br/social/search/software_infos?utf8=%E2%9C%93&utf8=%E2%9C%93&display=&filter=&software_type=public_software&query=celular&commit=Filtro&software_display=15&sort=


BRASIL
Simplifique!
Comunica BR
Participe
Acesso à informação
Legislação
Canais
Ir para o conteúdo 1
Ir para o menu 2
Ir para a busca 3
Ir para o rodapé 4
ACESSIBILIDADE
ALTO CONTRASTE
MAPA DO SITE
CADASTRE-SE
ENTRAR
Portal do
Software Público Brasileiro
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
Buscar no portal
Listas de discussão
Desenvolvimento
Social
Perguntas frequentes
Contato
CATÁLOGO DE SOFTWARE PÚBLICO
Resultado da pesquisa
PESQUISAR CATÁLOGO DE SOFTWARE
Todos
Software Público
forense
FILTRO
MAIS OPÇÕES
0 Software(s)
Exibir: 15
Ordenar por: Avaliação
Nenhum software encontrado. Tente outros filtros

9.1.14. Alguns softwares gratuitos são disponibilizados para análise forense, incluindo Autopsy/The Sleuth Kit, SANS Investigative Forensics Toolkit (SIFT), Mobile Verification Toolkit (MVT) e Android Debug Bridge (ADB).

9.1.15. **Autopsy/The Sleuth Kit**

9.1.15.1. O Autopsy é uma ferramenta de análise forense digital de código aberto, desenvolvida e mantida pelo U. S. Army Research Laboratory e pela empresa Basis Technology. Ele é utilizado para examinar dispositivos de armazenamento, como discos rígidos, SSDs e pen drives, a fim de recuperar e analisar evidências digitais. Há também suporte para análise de dispositivos móveis Android e iOS, a partir de cópias de dados fornecidos por outros sistemas forenses. Baseado no The Sleuth Kit (TSK), o Autopsy oferece uma interface gráfica que permite a inspeção de sistemas de arquivos, a recuperação de arquivos deletados, a análise de metadados e a identificação de artefatos digitais, como históricos de navegação, registros de mensagens e documentos acessados.

9.1.16. **SANS Investigative Forensics Toolkit (SIFT)**

9.1.16.1. O SANS Investigative Forensics Toolkit (SIFT) é um ambiente forense digital gratuito e de código aberto, desenvolvido pelo SANS Institute. Projetado para análise forense de computadores e resposta a incidentes, o SIFT é uma distribuição baseada no Ubuntu Linux que reúne um conjunto robusto de ferramentas especializadas para a investigação de sistemas de arquivos, análise de memória volátil, recuperação de dados deletados, detecção de malware e exame de logs de sistema. Ele inclui softwares como The Sleuth Kit (TSK), Volatility, Plaso e Rekall, permitindo a análise de evidências digitais.

9.1.17. **Mobile Verification Toolkit (MVT)**

9.1.17.1. O Mobile Verification Toolkit (MVT) é uma ferramenta de código aberto desenvolvida pela Amnesty International, voltada para a análise forense de dispositivos móveis, com foco especial na detecção de spyware e ameaças à segurança digital. O MVT permite examinar backups de iOS e dispositivos Android para identificar indicadores de comprometimento (IOCs), como registros de conexões suspeitas, arquivos maliciosos e anomalias nos metadados dos aplicativos.

9.1.18. **Avilla Forensics**

9.1.18.1. O Avilla Forensics é uma ferramenta para extração de dados e análise de dispositivos móvel gratuita. Foi criado em 2021 para auxiliar investigadores na coleta de informações e evidências de dispositivos móveis. Desenvolvida por Daniel Avilla, policial de São Paulo, a ferramenta fornece recursos avançados para extração lógica de dados e conversão de backup em formatos compatíveis com softwares de análise forense, como IPED e Cellebrite Physical Analyser.

9.1.18.2. Desde seu início, o Avilla Forensics recebeu atualizações significativas e possui módulos para extração de dados de Android, iOS, além de funcionalidades avançadas para extração de dados de aplicativos.

Solução 3: **Quanto ao desenvolvimento interno das soluções, destaca-se:**

9.1.19. **Indexador e Processador de Evidências Digitais (IPED)**

9.1.19.1. A Polícia Federal possui iniciativas voltadas ao desenvolvimento de soluções forenses, destacando-se o Indexador e Processador de Evidências Digitais (IPED). Inicialmente concebido para indexar relatórios do FTK 1.8 (convertidos pelo AsAP3) e do FTK 3+, o IPED evoluiu significativamente, incorporando funcionalidades que permitem sua integração com outras ferramentas comerciais. Atualmente, ele é amplamente utilizado nos laboratórios das Unidades de Criminalística para análise de evidências digitais.

9.2. ANÁLISE COMPARATIVA DAS SOLUÇÕES

9.2.1. Quanto aos requisitos definidos no Art. 11, inciso II, da IN SGD/ME n. 94/2022.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	

	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

9.2.2. Quanto aos Requisitos de Negócio

Requisitos de Negócio		Soluções								
		1- Aquisição de software forense				2- Softwares Livres/gratuitos				3- Desenvolvimento interno (IPED)
Id	Descrição	Cellebrite Physical Analyzer	Magnet Axiom	Oxygen Forensic Detective	MSAB Analyze – XAMN	Autopsy/The Sleuth Kit	SANS Investigative Forensics Toolkit (SIFT)	Mobile Verification Toolkit (MVT)	Avilla Forensics	

RN1	Decodificação e interpretação de dados de extração de computadores e celulares	PARCIALMENTE	ATENDE	ATENDE	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE	ATENDE
RN2	Suporte para múltiplos dispositivos em uma mesma visão, com o objetivo de realizar uma análise integrada entre as evidências apreendidas	ATENDE	ATENDE	ATENDE	PARCIALMENTE	NÃO ATENDE	NÃO ATENDE	NÃO ATENDE	NÃO ATENDE	ATENDE
RN3	Suporte aos sistemas operacionais Windows, macOS e Linux	PARCIALMENTE	ATENDE	ATENDE	NÃO ATENDE	ATENDE	PARCIALMENTE	NÃO ATENDE	NÃO ATENDE	ATENDE
RN4	Suporte aos sistemas operacionais iOS e Android	ATENDE	ATENDE	ATENDE	ATENDE	PARCIALMENTE	NÃO ATENDE	PARCIALMENTE	ATENDE	PARCIALMENTE
RN5	Decodificação e análise de dados provenientes de nuvem	ATENDE	ATENDE	ATENDE	PARCIALMENTE	NÃO ATENDE	NÃO ATENDE	NÃO ATENDE	NÃO ATENDE	PARCIALMENTE
RN6	Suporte a ferramentas que auxiliem na análise de casos envolvendo abuso sexual infantil	ATENDE	ATENDE	ATENDE	ATENDE	PARCIALMENTE	PARCIALMENTE	NÃO ATENDE	NÃO ATENDE	ATENDE
RN7	Direito de atualização e suporte técnico por 36 meses	ATENDE	ATENDE	ATENDE	ATENDE	NÃO SE APLICA	NÃO SE APLICA	NÃO SE APLICA	NÃO SE APLICA	NÃO SE APLICA
RN8	Suporte técnico (8X5)	ATENDE	ATENDE	ATENDE	ATENDE	NÃO ATENDE	NÃO ATENDE	NÃO ATENDE	NÃO SE APLICA	NÃO ATENDE
RN9	Compatibilidade com a Arquitetura Tecnológica dos laboratórios forenses da Polícia Federal.	ATENDE	ATENDE	ATENDE	ATENDE	ATENDE	NÃO ATENDE	NÃO ATENDE	ATENDE	ATENDE

9.2.2.1. No que se refere as ferramentas gratuitas, embora algumas soluções ofereçam funcionalidades básicas de análise de discos, sistemas de arquivos e dispositivos móveis, elas apresentam restrições em relação às necessidades estabelecidas neste Estudo Técnico Preliminar (ETP). As principais limitações incluem suporte

limitado a dispositivos móveis, a ausência de um mecanismo integrado para comparação de *hashes* com bases especializadas, como Project VIC, utilizados em investigações criminais; a falta de um algoritmo automatizado para detecção de nudez, armas e substâncias proscritas em imagens e vídeos; ausência de suporte nativo para identificação de carteiras, chaves privadas ou análise de transações em blockchain, o que limita sua utilidade para investigações envolvendo criptomoedas; ausência de suporte adequado à decodificação e análise de dados armazenados na nuvem, funcionalidade útil para recuperação estruturada de backups de iCloud ou Google Drive; e a fragmentação entre diferentes ferramentas, tornando o fluxo de trabalho menos eficiente e aumentando a complexidade operacional.

9.2.2.2. Diante dessas limitações, as ferramentas gratuitas analisadas não atendem integralmente aos requisitos estabelecidos neste Estudo Técnico Preliminar (ETP).

9.2.2.3. Sobre as soluções comerciais, o MSAB Analyze - XAMN, apesar de possuir funcionalidades avançadas de análise de dados extraídos de dispositivos móveis, não oferece suporte adequado para a análise forense de evidências provenientes de computadores. Isso representa uma limitação significativa, considerando que a ferramenta a ser contratada deve ser capaz de processar e interpretar dados de múltiplas fontes, incluindo Windows, macOS e Linux, garantindo uma abordagem forense completa e integrada.

9.2.2.4. O Cellebrite Inseyets Physical Analyzer 10 ampliou suas capacidades para incluir a análise de dados de sistemas Windows, atendendo parcialmente ao requisito de suporte a múltiplos sistemas operacionais. No entanto, para garantir uma cobertura completa que inclua macOS, seria necessário utilizar o Cellebrite Inspector. Além disso, não há suporte explícito para Linux em nenhuma das ferramentas da Cellebrite, o que indica que, para atender integralmente aos requisitos de análise de artefatos de Windows, macOS e Linux, seria necessário considerar soluções adicionais ou complementares que proporcionem suporte abrangente a esses sistemas operacionais.

9.2.2.5. As soluções da Cellebrite já são amplamente utilizadas pela Polícia Federal, sendo ferramentas fundamentais para investigações forenses. No entanto, este projeto visa a aquisição de uma segunda ferramenta, com o objetivo de ampliar a capacidade de análise forense e aprimorar a identificação de evidências, garantindo um ambiente mais robusto para a investigação criminal. Essa abordagem está alinhada às boas práticas forenses, que recomendam o uso de mais de uma ferramenta forense nos laboratórios, permitindo correlação de dados, validação de resultados e maior confiabilidade nas análises.

9.2.2.6. Quanto ao desenvolvimento interno do IPED (solução 3), destaca-se que se trata de uma ferramenta essencial na busca e análise de evidências provenientes de mídias de armazenamento, como HDDs, SSDs, cartões de memória, pen drivers, além de permitir a integração com relatórios gerados por softwares de extração de dados de dispositivos móveis.

9.2.2.7. No entanto, o IPED não possui capacidade nativa para processar e estruturar dados provenientes de serviços em nuvem, como, por exemplo, a garantia de retorno de mandado de nuvem dos principais provedores, bem como suporte limitado para decodificar dados brutos extraídos de dispositivos móveis. Para essas finalidades, ele depende dos relatórios gerados por ferramentas proprietárias, como aquelas da Cellebrite, especificamente no formato UFDR. Embora o IPED forneça uma interface diferenciada para visualização desses dados e permita o uso de *parsers* próprios para busca de novas evidências, por vezes, sua funcionalidade está condicionada ao pré-processamento realizado por soluções comerciais.

9.2.2.8. Neste sentido, para desenvolver uma solução que atenderia todos os requisitos deste ETP, devido à alta complexidade técnica, seria necessária uma equipe dedicada e permanente, pois a evolução do software seria contínua e requer atualizações frequentes para acompanhar mudanças nos sistemas operacionais, dispositivos e protocolos de comunicação. A manutenção e aprimoramento dessas ferramentas exigiriam recursos significativos

e um esforço ininterrupto de engenharia reversa e desenvolvimento. Entretanto, não faz parte do core business da Polícia Federal desenvolver internamente esse tipo de software, considerando sua missão institucional e sua natureza de polícia judiciária da União.

9.2.2.9. Pelos motivos expostos, o desenvolvimento interno de uma solução que atenda integralmente os requisitos deste processo não é viável.

9.2.3. Quanto aos Requisitos Tecnológicos

9.2.3.1. A análise dos requisitos de negócio identificou que as soluções 2 e 3 não atendem as necessidades deste processo. Sobre a solução 1 (ferramentas comerciais), duas delas se destacaram por atenderem a todos os requisitos macros de negócio, devendo ser analisadas no detalhe quanto aos requisitos técnicos.

9.2.3.2. Com essa premissa, a seguir são analisadas estas ferramentas forenses comerciais, considerando com base a documentação técnica e informações localizadas prioritariamente em seus sites ou de *release notes* de ferramentas já em uso na PF. A documentação que embasou a análise dos requisitos de negócios e tecnológicos consta consignada no documento SEI 143057578.

ID	Descrição	Solução 1 - Aquisição de software forense	
		Magnet Axiom	Oxygen Detective
RT1	Possuir suporte à decodificação de dados de dispositivos móveis, HDD, SSD, dispositivos USB e pastas de arquivos	ATENDE	ATENDE
RT2	Permitir a decodificação de dados de sistemas operacionais Windows, macOS, Linux	ATENDE	ATENDE
RT3	Permitir a decodificação de dados de dispositivos móveis com sistema operacional Android, e iOS	ATENDE	ATENDE
RT4	Gerar relatórios nos formatos XML, HTML, CSV ou XLS, PDF e em formato portátil	ATENDE	ATENDE
RT5	Permitir o cálculo de HASH MD5 e SHA-256	ATENDE	ATENDE
RT6	Permitir realizar pesquisas utilizando textos, keyword, REGEX e GREP	ATENDE	ATENDE
RT7	Permitir realizar a decodificação e análise dos dados utilizando uma única plataforma	ATENDE	ATENDE
RT8	Permitir aplicação de filtros para auxiliar a pesquisa por artefatos	ATENDE	ATENDE
RT9	Permitir realizar a marcação de arquivos por meio de tags	ATENDE	ATENDE
RT10	Permitir gerar visualização utilizando Timeline	ATENDE	ATENDE
RT11	Permitir visualizar dados que possuem dados geográficos no mapa (geolocalização)	ATENDE	ATENDE

RT12	Permitir realizar uma pré-visualização dos arquivos analisados em uma mesma interface	ATENDE	ATENDE
RT13	Permitir visualizar os arquivos no formato Hexadecimal para uma análise mais detalhada dos dados	ATENDE	ATENDE
RT14	Permitir a exportação dos dados encontrados no arquivo de evidência	ATENDE	ATENDE
RT15	Permitir a recuperação de arquivos deletados e não sobrescritos	ATENDE	ATENDE
RT16	Permitir colaboração e compartilhamento de evidências	ATENDE	ATENDE
RT17	Permitir recuperar o Backups do iTunes	ATENDE	ATENDE
RT18	Permitir recuperar informações quando um arquivo de torrent foi criado, modificado e baixado	ATENDE	ATENDE
RT19	Permitir busca por palavra-chave em sistema de arquivos	ATENDE	ATENDE
RT20	Permitir analisar artefatos P2P em dispositivos Android	ATENDE	NÃO IDENTIFICADO
RT21	Permitir verificação baseada em Hash de imagem forense E01	ATENDE	ATENDE
RT22	Possuir interface em no mínimo Inglês ou Português – Brasileiro	ATENDE	ATENDE
RT23	Permitir a inserção da chave de criptografia de um disco criptografado com BitLocker antes do processamento do mesmo	ATENDE	ATENDE
RT24	Permitir a criação de perfis de artefatos para diferentes tipos de casos	ATENDE	ATENDE
RT25	Possuir a capacidade de realizar o correlacionamento dos dados	ATENDE	ATENDE
RT26	Possuir funcionalidade de Inteligência Artificial para auxiliar na identificação de evidências, com suporte para interações em linguagem natural através de assistente virtual (chat).	ATENDE	NÃO IDENTIFICADO
RT27	Suporte a Imagens forenses de evidências no mínimo com os seguintes formatos de arquivo: E01, Ex01, L01, Lx01, AD1, dd, raw, bin, img, dmg, vmdk, vhd, vdi, xva, ufd, ufdx, zip, tar;	ATENDE	ATENDE
RT28	Suporte para decodificação e análise de dados extraídos com as ferramentas forenses Cellebrite Inseyts e Magnet GrayKey	ATENDE	ATENDE
RT29	Suporte aos sistemas de arquivos: NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2, APFS	ATENDE	ATENDE
RT30	Detecção automática de criptografia Truecrypt, Bitlocker, PGP, e Safeboot	ATENDE	PARCIAL

RT31	Capacidade de pré-visualização de arquivos plist	ATENDE	ATENDE
RT32	Capacidade de pesquisa do espaço não alocado em uma imagem APFS	ATENDE	NÃO IDENTIFICADO
RT33	Suporte de análise para itens recuperados de $RECYCLE.BIN	ATENDE	ATENDE
RT34	Permitir a decodificação e análise da dados capturados de memória RAM	ATENDE	ATENDE
RT35	Permitir a comparação de hashes com bases especializadas, como Project VIC	ATENDE	ATENDE
RT36	Capacidade de análise de retorno de mandados judiciais de dados provenientes de nuvens, considerando ao menos Instagram, Facebook, Snapchat, Twitter, Google e Apple.	ATENDE	ATENDE
RT37	Uso de tokens extraídos da memória de aparelho celular para acesso a serviços e cópia forense de dados de serviços com armazenamento de dados na nuvem, contornando o segundo fator de autenticação, se necessário.	ATENDE	ATENDE
RT38	Localização e extração de tokens do computador (Windows, macOS)	ATENDE	ATENDE
RT39	Reconstrução de páginas WEB	ATENDE	ATENDE
RT40	Recuperação de dados públicos de redes sociais	ATENDE	NÃO ATENDE
RT41	Suporte fontes com duplo fator de autenticação	ATENDE	ATENDE
RT42	Permitir agregar várias fontes de dados em um único caso	ATENDE	ATENDE
RT43	Permiti detectar automaticamente possíveis imagens de conteúdo ilícito, como abuso infantil, substâncias proscritas e armas.	ATENDE	ATENDE
RT44	Permitir a identificação de carteiras, chaves privadas e análise de transações em blockchain, auxiliando em investigações envolvendo criptomoedas	ATENDE	ATENDE
RT45	Visualização de SQLite	ATENDE	ATENDE
RT46	Visualização em formato Hexadecimal	ATENDE	ATENDE
RT47	Visualização de geolocalização em mapas	ATENDE	ATENDE
RT48	Definir e alterar fuso horário padrão	ATENDE	ATENDE
RT49	Customização de relatórios	ATENDE	ATENDE

RT50	Recuperação de imagens, localizações, strings e demais arquivos apagados (carving)	ATENDE	ATENDE
RT51	Tratamento de banco de dados de aplicativos não categorizados, através do banco de dados (Assistente do SQLite)	ATENDE	NÃO IDENTIFICADO
RT52	Geração de dicionário de palavras e números, para ser utilizado como referência de ataque para quebra de senha	ATENDE	NÃO IDENTIFICADO
RT53	Customização e execução de scripts Python	ATENDE	NÃO IDENTIFICADO
RT54	Permitir atualização e suporte técnico por 36 meses	ATENDE	ATENDE
RT55	Fornecer Suporte técnico (8X5)	ATENDE	ATENDE
RT56	Compatibilidade com a arquitetura tecnológica dos laboratórios forenses de informática, com Workstations baseadas prioritariamente em Sistemas Operacionais Windows	ATENDE	ATENDE

Atende: o software tem como objetivo geral o atendimento a uma das necessidades de negócio e foi identificada a funcionalidade que atende ao requisito tecnológico.

Não atende: o software não tem como função geral o atendimento de uma necessidade de negócio ou uma necessidade técnica específica.

Parcial: o software tem como objetivo atender a uma necessidade de negócio, mas não atende todos os requisitos técnicos de forma abrangente.

Não identificado: o software tem como objetivo geral o atendimento de uma necessidade de negócio, mas não foi possível identificar se o software atende ao requisito tecnológico.

10. Registro de soluções consideradas inviáveis

10.1. Após análises apresentadas na Seção 9, foram considerados inviáveis os cenários apresentados nas Soluções 2 e 3. Portanto, a única solução que atende todos os requisitos definidos neste ETP pela área demandante e é viável é a Solução 1 (Contratação de ferramenta pericial para análise de vestígios digitais relacionados a computadores (discos rígidos) e aparelhos celulares). Entre as ferramentas de mercado objeto de estudo, a única que atende todos os requisitos de negócios e tecnológicos é a ferramenta Magnet Axiom.

10.2. No Brasil, há um único representante comercial especialista e autorizado pelo fabricante para fornecimento e suporte técnico aos seus produtos nesta Região – a TechBiz Forense Digital Ltda, conforme atesta a Certidão Nº 250904/44.169 (Documento SEI 143061704).

10.3. Portanto, mediante esse cenário de exclusividade e com base na comparação técnica disposta na análise das soluções constante no item 9, justifica-se tecnicamente a contratação por inexigibilidade de licitação do Objeto deste ETP, com fundamento no art. 74, inciso I, da Lei nº 14.133, de 1º de abril de 2021.

11. Análise comparativa de custos (TCO)

11.1. TCO, do inglês Total Cost of Ownershsip, custo total de propriedade é um método utilizado para calcular o custo global de um produto ou serviço ao longo de seu ciclo de vida, considerando custos diretos e indiretos.

11.2. Utiliza-se esse conceito para se referir à estimativa dos custos dos cenários projetados ao longo do uso da solução, possibilitando uma análise mais precisa e abrangente economicamente. Por conseguinte, é necessário estimar os custos de bens e serviços para cada cenário viável. Assim sendo, recomenda-se utilizar os mecanismos previstos na IN Seges/ME nº 65/2021.

11.3. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Solução 1 – Licenças Magnet Axiom
Custo Total de Propriedade – Memória de Cálculo
O custo total previsto, referente ao projeto, é de R$ 3.894.780,00 (três milhões, oitocentos e noventa e quatro mil e setecentos e oitenta reais). Nele estão incluídos os softwares e demais componentes, com licenciamento por subscrição; garantia de atualização tecnológica do fabricante e serviço de suporte técnico remoto do fornecedor Techbiz, por 36 meses; serviços básicos de instalação e configuração; além de suporte técnico remoto do fornecedor TechBiz. No caso em questão, por se tratar de um software com instalação direta nas workstations dos laboratórios de perícia, não há custos com adaptação de instalações físicas, as quais já se encontram plenamente operacionais para as atividades ordinárias de perícia (computador, rede de dados, rede elétrica, mobiliário, etc).

O maior custo agregado ao processo é o de licenciamento das ferramentas sob a modalidade de subscrição. Nessa modalidade, outros custos como a manutenção do software, que inclui custos de desenvolvimento e de pessoal, ficam a cargo do fornecedor.

Os valores de referência têm como base a pesquisa de mercado com memória de cálculo consolidada na Nota Técnica SEI n. 143062545.

11.4. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	**Estimativa de TCO ao longo dos anos**			**Total**
	Ano 2025	Ano 2026	Ano 2017	
Magnet Axiom Advanced	R$ 1.298.260,00	R$ 1.298.260,00	R$ 1.298.260,00	**R$ 3.894.780,00**

12. Descrição da solução de TIC a ser contratada

12.1. DETALHAMENTO DO MODELO DE LICENCIAMENTO PAGAMENTO

12.1.1. O software Magnet Axiom Advanced é atualmente fornecido através de modelo de licenciamento por subscrição. O modelo de licenciamento de software por subscrição é uma forma de comercialização em que o

contratante paga um valor recorrente para ter direito ao uso do software durante o período contratado. Diferente da licença perpétua, em que o cliente paga uma vez e possui o direito indefinido de uso da versão adquirida, a subscrição funciona como um serviço: enquanto o pagamento é mantido, o usuário tem acesso não apenas ao software, mas também a atualizações, correções, novos recursos e suporte técnico. Esse modelo proporciona previsibilidade de custos, reduz desembolsos iniciais e garante que a contratante utilize sempre a versão mais atual e do software.

12.1.2. Por intermédio da carta SEI n. 143061461, o fornecedor esclareceu que "(…) o produto Magnet Axiom, antes comercializado na forma de licenciamento perpétuo, é, em tempos recentes, tão **somente licenciado e comercializado sob a forma de licenciamento por tempo determinado (subscrição anual)**, tendo o mesmo sido determinado por seu referido fabricante, por seu direito exclusivo. (…)." (grifo nosso).

12.1.3. Sobre a forma de pagamento, cabe esclarecer que a portaria SGD/MGI nº 5.950/2023, que estabelece modelo de contratação de software a ser seguido por órgãos do Poder Executivo Federal, estabelece que "excepcionalmente, admite-se o pagamento antecipado para remuneração por créditos se constatado que a solução propiciará sensível economia de recursos ou representará condição indispensável para a prestação do serviço, hipóteses que deverão ser previamente justificadas no estudo técnico preliminar por meio de memória de cálculo específica".

12.1.4. Neste sentido, foram realizadas análises de contratos firmados entre entidades da Administração Pública e o representante comercial da fornecedora dos serviços no Brasil, listados a seguir:

- Contrato DIPOL PC/SP Nº 03/2025 (SEI n. 143059037);
- Contrato PM/SP Nº 13791/260/2024 (SEI n. 143059066)
- Contrato SEJUSP/MS Nº 026/2025 (SEI n. 143059077)
- Contrato SEPOL/RJ Nº 063/SEPOL/2024 (SEI n. 143059586)

12.1.5. Estes contratos têm vigência definidas para 12 ou 36 meses. Em análise, para todos os contratos a forma de pagamento é anual ou o valor total do contrato.

12.1.6. Além do estudo de mercado a partir de contratos firmados com entes públicos, foi solicitado esclarecimento ao fornecedor quanto ao modelo de pagamento das soluções da Magnet. Em resposta, o fornecedor encaminhou carta SEI n. 143061456 em que esclarece que o fabricante apenas pratica o modelo de licenciamento com métricas anuais, afirmando que se trata de prática adotada em todos os contratos públicos celebrados com os Órgãos de Forças da Lei e de Segurança Pública do governo brasileiro, ratificando o cenário já observado durante a pesquisa de mercado por meio dos contratos analisados.

12.1.7. Além disso, conforme Portaria SGD/MGI nº 5.950/2023, o contrato a ser firmado poderá ter vigência de até 5 (cinco) anos, nas hipóteses de serviços e fornecimentos contínuos, podendo ser prorrogado, até o limite de 10 (dez) anos, conforme as regras e diretrizes estabelecidas nos arts. 105 a 107 da Lei nº 14.133, de 2021.

12.1.8. A definição da vigência do contrato deve considerar aspectos técnicos e econômicos do objeto, devidamente registrados nos Estudos Técnicos Preliminares pela equipe de planejamento da contratação.

12.1.9. Ao ponderar sobre a forma de pagamento anual definida no modelo de negócio da contratante e constatada nos diversos contratos analisados, chega-se à conclusão de que o pagamento anual, em um contrato com vigência de 36 meses, apresenta vantagens para a Polícia Federal.

12.1.10. Essa modalidade proporciona uma gestão orçamentário-financeira mais eficiente, uma vez que reduz o desembolso financeiro inicial significativamente, além de respeitar o princípio da anualidade do orçamento.

12.1.11. Além disso, o parcelamento do valor a ser pago em parcelas anuais permite uma maior flexibilidade financeira e favorece a atuação do gestor público na administração orçamentária ao não comprometer excessivamente o orçamento total disponibilizado em Lei para o órgão. Isso contribui para uma alocação de recursos de forma mais estratégica e eficaz, considerando que há necessidade de gerir o orçamento total de forma equilibrada, observando outras demandas prioritárias.

12.1.12. Outra vantagem do pagamento por ano está relacionada à gestão contratual. Com essa abordagem, a Administração tem a oportunidade de aplicar instrumentos de gestão contratual de forma mais eficiente. Pode realizar avaliações regulares dos níveis de serviço fornecidos, e, caso necessário, reter pagamentos, aplicar multas, glosas e outras sanções de maneira mais oportuna e precisa. Isso contribui para um melhor controle e monitoramento do contrato ao longo do tempo, garantindo o cumprimento de todas as cláusulas e requisitos a serem definidos em contrato.

12.1.13. Portanto, ao adotar o modelo de pagamento anual, em uma proposta contratual de 36 meses, a Polícia Federal obtém uma série de benefícios, incluindo gestão orçamentária mais eficiente, flexibilidade financeira, melhor aplicação de instrumentos de gestão contratual e simplificação dos processos administrativos, lembrando, ainda, que há impossibilidade de contratar junto ao fornecedor um modelo alternativo de pagamento mensal ou sob demanda.

12.1.14. Quanto a economicidade, cabe ressaltar que não é possível a comparação de preços do modelo de pagamento anual, frente a pagamento sob demanda, ou mensal, considerando que não há esse modelo de licenciamento e pagamento mensal ofertado pela contratante, conforme já demonstrado.

12.1.15. Ainda assim, a análise de preços consolidada na Nota Técnica SEI n. 143062545 demonstrou uma vantajosidade da Proposta Comercial 143061933, com uma redução e valor estimada em cerca de 23% frente a pesquisa de preços, conforme tabela a seguir:

Mapa Comparativo de Preços de Contratos Similares VS Propostos – Valor de Referência - Valor Global							
Item	**Descrição**	**Prazo**	**Qnd**	**Preço unitário da pesquisa para 36 meses**	**Valor total da pesquisa para 36 meses**	**Valor Unitário proposto para 36 meses**	**Valor total proposto**
1	Ferramenta pericial para análise de computadores e aparelhos celulares (Magnet Axiom Advanced - Licenciamento Dongle). Licença de uso na modalidade Subscrição com garantia, atualização e suporte técnico inclusos	36 meses	20	R$ 252.643,53	R$ 5.052.870,60	R$ 194.739,00	**R$ 3.894.780,00**
Demonstrativo da economicidade (para 36 meses)							
Valor Global de Referência (A)							R$ 5.052.870,60
Valor Global da Proposta Comercial (B)							R$ 3.894.780,00
Diferença (C = A – B)							**R$ 1.158.090,60**

Percentual de economia de recursos (C/A)	**22,9%**

13. Estimativa de custo total da contratação

Valor (R$): 3.894.780,00

13.1.A expectativa do custo total da solução, para 36 (trinta e seis) meses, é de R$ 3.894.780,00 (três milhões, oitocentos e noventa e quatro mil, setecentos e oitenta reais), com desembolso tal como segue:

Momento	Item	Catser	Valor
Após Assinatura do Contrato	Subscrição de software para o Ano 2025	27502	R$ 1.298.260,00
Após 12 meses da assinatura do contrato	Subscrição de software para o Ano 2026	27502	R$ 1.298.260,00
Após 24 meses da assinatura do contrato	Subscrição de software para o Ano 2027	27502	R$ 1.298.260,00
Total			R$ 3.894.780,00

13.2. Registra-se que os valores de referência têm como base a pesquisa de mercado com memória de cálculo consolidada na Nota Técnica SEI n. 143062545.

14. Justificativa técnica da escolha da solução

14.1. Diante da análise realizada, resta evidenciado que o Magnet Axiom atende integralmente aos requisitos técnicos e de negócios estabelecidos neste Estudo Técnico Preliminar, mostrando-se compatível com o parque tecnológico da Polícia Federal e incorporando recursos avançados de decodificação e análise de dados. Considerando a heterogeneidade de dispositivos e formatos de informações com que se deparam os exames periciais, verifica-se que a solução em apreço se configura como a alternativa mais adequada do ponto de vista técnico, por ampliar a eficiência, a abrangência e a precisão dos resultados. Assim, diante do exposto, conclui-se pela viabilidade da contratação das licenças do referido software, por atender às necessidades institucionais e fortalecer a estratégia de utilização de soluções complementares no âmbito dos exames periciais.

14.2. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.2.1. A IN SGD/ME nº 94, de 2022, art. 12, inciso I, define que é necessário realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viável e economicamente

vantajoso, observado o disposto nos §§ 2º e 3º do art. 40 e § 1º do art. 47 da Lei nº 14.133, de 2021, justificando-se a decisão de parcelamento ou não da solução.

14.2.2. No caso concreto, a análise deste ETP definiu como solução viável a contratação da ferramenta Magnet Axiom, em modelo de subscrição, que é uma solução única não passível de parcelamento.

14.2.3. Pelo exposto, a equipe de planejamento da contração define pelo não parcelamento da contratação.

15. Justificativa econômica da escolha da solução

15.1. Das soluções apresentadas, houve apenas uma viável, pois atendeu aos requisitos técnicos e de negócios. Logo, o principal critério na escolha da solução foi o técnico.

15.2. Do ponto de vista econômico, foi realizada uma ampla pesquisa de mercado, conforme disposto na Nota Técnica SEI n. 143062545, o que definiu a solução como economicamente vantajoso.

16. Benefícios a serem alcançados com a contratação

16.1. O atendimento da demanda constante no presente processo, propiciará à esta área requisitante:

16.1.1. Atingir dados contidos em dispositivos móveis, agilizando os processos persecutórios, a melhoria na tomada de decisões investigativas e sobre redirecionamento estratégico;

16.1.2. Proporcionar maior eficiência nas ações de combate ao crime organizado, por meio do emprego eficiente dos recursos disponíveis;

16.1.3. Alcance de informações delituosas salvaguardadas e de relevância processual;

16.1.4. Prover os recursos necessários para que as unidades de criminalísticas possam obter a materialização de crimes e subsidiar uma eventual condenação de envolvidos que tentam ocultar as evidências;

17. Providências a serem Adotadas

17.1. Quanto a definição de ações para viabilizar a possível substituição da solução a ser contratada:

17.1.1. Conforme subitem 1.4.1 do Anexo I da IN SGD/ME nº 94, de 2022, no ETP deve-se “Avaliar e definir ações para viabilizar a possível substituição da solução a ser contratada adotando medidas que minimizem a dependência tecnológica, a exemplo da adoção de padrões tecnológicos comuns de mercado ou padrões abertos e da previsão de serviços e funcionalidades de migração”.

17.1.2. Conforme detalhado ao longo da análise das soluções, não foi identificada solução de mercado com padrões abertos. Além disso, trata-se de um software proprietário que não prevê em seu modelo de negócio a disponibilização de código fonte ou processo de cessão de tecnologia.

17.1.3. Trata-se de uma solução que demanda um conhecimento especializado e de restrito acesso, inclusive, com um único fornecedor. Neste sentido, cabe à DITEC realizar constantes estudos e prospecções de novas tecnologias e, em momentos como a realização de um novo contrato, observar se há evoluções nas ferramentas de mercado que possibilitem a substituição da tecnologia que se pretende contratar neste processo.

17.2. Quanto a capacitação de servidores para fiscalização contratual

17.2.1. Informa-se que os servidores indicados para compor a Equipe de Planejamento da Contratação (EPC) possuem amplo conhecimento quando as ferramentas forenses e investigativas objeto deste processo, devendo realizar o repasse de conhecimento aos fiscais, caso seja designado outros servidores que não compuseram a EPC. Além disso, a fiscalização do contrato deverá ser regida pela IN SGD/ME n. 94/2022, art. 2º, inciso V, que define uma equipe multidisciplinar incluindo integrantes técnicos e administrativos com conhecimentos adequados à fiscalização contratual.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1. Com base nos elementos técnicos apresentados neste Estudo Técnico Preliminar, a contratação por inexigibilidade do software forense Magnet Axiom se mostra uma solução viável e indispensável. A ferramenta atende às necessidades de decodificação e análise de dados provenientes de dispositivos móveis e sistemas computacionais em nuvem, que frequentemente constituem a única evidência material em crimes de alta complexidade.

18.2. Diante desse cenário, e considerando os benefícios de uma abordagem que utiliza múltiplas soluções complementares para garantir a robustez dos resultados periciais, a Equipe de Planejamento da Contratação declara VIÁVEL a aquisição da solução Magnet Axiom, conforme as necessidades apontadas pela área demandante, registradas no Documento de Formalização da Demanda.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

LUIS FILIPE DA CRUZ NASSIF

Integrante Requisitante Titular

Assinou eletronicamente em 27/11/2025 às 17:34:09.

TIAGO BARROSO DE MELO

Integrante Requisitante Substituto

Assinou eletronicamente em 27/11/2025 às 14:54:28.

RICARDO RIBEIRO MENDES

Integrante Técnico Titular

Assinou eletronicamente em 27/11/2025 às 14:43:59.

IGOR HEIDRICH

Integrante Técnico Substituto

Assinou eletronicamente em 01/12/2025 às 18:39:02.

ROBERTO REIS MONTEIRO NETO

Autoridade competente

Assinou eletronicamente em 01/12/2025 às 19:04:06.