



SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
INSTITUTO NACIONAL DE CRIMINALÍSTICA - INC/DITEC/PF

Estudo Técnico Preliminar da Contratação

Processo nº 08201.001459/2019-94

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Processo nº 08201.001459/2019-94

O presente documento tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. Dados do Processo:

Órgão Responsável pela contratação:	DIRETORIA TÉCNICO-CIENTIFICA - POLÍCIA FEDERAL
Objeto:	Renovação de softwares periciais na área de Informática (IEF/Axiom e FTK)
Nº do Processo:	08201.001459/2019-94
Equipe de Planejamento:	Rosemeire Abadia Moreira - Perito Criminal Federal Elcio Ricardo de Carvalho - Perito Criminal Federal Claudinete Tavares Firmino - Agente Administrativo

2. Planejamento Estratégico:

A presente contratação visa renovar licença das ferramentas periciais IEF/Axiom e FTK (Forensic Toolkit) que se encontram com as licenças vencidas. A renovação se dá de forma a manter a capacidade de análise e decodificação de dados presentes em mídias de armazenamento computacional submetidas à perícia no Instituto Nacional de Criminalística e nos Setores, Unidades e Núcleos Técnicos-Científicos em todo o território nacional.

O SEPINF - Serviço de Perícias em Informática tem como atribuição, entre outras: realizar exames periciais em material envolvendo crime por computador e outros crimes congêneres cometidos com o emprego de recursos de informática, nos termos da Instrução Normativa nº 13/2005. Para bem se desincumbir de sua Missão, a unidade se organiza em 05 (cinco) frentes, a saber: realiza procedimentos periciais; desenvolve soluções em informática forense; gerencia projetos informáticos; promove capacitação na área que atua; realiza Gestão Estratégica. Deste modo, forma-se um arcabouço de atividades que busca atender à demanda e prospectar novas tecnologias de combate ao crime informático, no que diz respeito à atividade pericial.

As necessidades de negócio emergem da evolução natural da tecnologia da informação, a qual

é a matéria-prima para o desenvolvimento de soluções do SEPINF, afinal, cuida de analisar material de informática apreendido em local de crime, entre outros, por determinação judicial. Logo, é de se buscar meios céleres para a boa consecução deste mister. Ocorre que no cometimento de crimes é comum que o criminoso realize condutas, as quais para serem bem elucidadas devem ser submetidas a avaliação extensiva, tanto mais quando a tecnologia oferece mecanismos que dificultam a ação do Estado, a exemplo de senhas, acesso a dispositivos por biometria, bloqueio de equipamentos, armazenamento à distância de dados (ex.: nuvens computacionais), criptografia entre outros.

Ocorre que essa atividade deixa vestígios, portanto, o Perito Criminal Federal deve assenhorar-se de um conjunto de técnicas e procedimentos, aceitos internacionalmente, para defender, extrair e apresentar elementos de interesse pericial, disponíveis em dispositivos computacionais integrantes de material de informática objeto do trabalho dos Peritos. Nesse sentido, é da própria tecnologia que há de se buscar solução para essa área negocial do SEPINF, ou seja, não há solução fora da tecnologia, portanto, este Estudo vai direto ao ponto, avaliando possibilidades no campo da informática forense.

A presente proposta de contratação visa a atender a área de procedimentos periciais e colabora com a área Desenvolvimento de Soluções. Portanto, o estudo avalia as três principais ações típicas que são comuns na contratação de softwares: a) verificar a existência de software livre, público ou gratuito que atenda aos requisitos requeridos; b) desenvolver internamente, sob execução direta, um software que atenda aos requisitos requeridos e c) adquirir software de mercado que atenda aos requisitos requeridos. Ao decidir sobre qual solução adotar, é imperioso considerar que os serviços adquiridos vão ser aplicados em solução que já é parte do arcabouço de soluções em uso no SEPINF, o que inclui ferramentas já desenvolvidas sob execução direta.

A ação alinha-se com o Objetivo Estratégico da Diretoria Técnico-Científica da Polícia Federal no tocante aos eixos "gerenciar, manter e atualizar o parque tecnológico", "manter-se na vanguarda do conhecimento científico aplicado às Ciências Forenses" e "apresentar excelência na qualidade da prova".

As despesas decorrentes desta aquisição correrão à conta dos recursos consignados no Orçamento Geral da União para o exercício de 2020, a cargo da Diretoria Técnico-Científica da Polícia Federal.

3. Requisitos da Contratação:

3.1. Justificativa da Contratação:

A contratação de solução na área de recuperação e extração de artefatos computacionais armazenados em mídias digitais se revela fundamental, na medida em que não há previsão de desenvolvimento próprio de soluções dessa natureza no SEPINF, por razões que se pode listar da seguinte maneira: a) o custo envolvido não é totalmente claro, podendo chegar facilmente a valores maiores do que das soluções de interesse. O investimento deveria ser constante, porque com a evolução de produtos oferecidos pelo mercado de tecnologia da informação, de igual modo a solução deveria evoluir, porém, não há previsão de que a Polícia Federal se torne autossuficiente em desenvolvimento de software próprio, para todas as áreas em que o SEPINF atua, notadamente, quanto a extração de dados dos dispositivos legalmente apreendidos. b) não há previsão de que a Polícia Federal crie uma unidade que seja capaz de lidar com todas as etapas do desenvolvimento de softwares para informática forense, considerando a natureza de polícia judiciária da União do órgão; portanto, o desenvolvimento atual é pontual e direcionado para atender a requisitos que não dependem de investimentos vultosos em pessoal, suporte técnico e manutenção dos produtos desenvolvidos.

A realização dos exames demandados aos Peritos Criminais Federais depende da utilização de ferramentas especializadas cujas licenças costumam ser renovadas a cada 3 anos. As ferramentas contempladas neste Estudo Técnico Preliminar são:

- Forensic Toolkit (FTK): Software especializado em recuperação e extração de dados e artefatos armazenados em mídias digitais. Licenças vencidas em dezembro/2018;
- IEF/Axiom: Software especializado em recuperação e extração de dados e artefatos armazenados em mídias digitais. Licenças vencidas em fevereiro/2019;

Cotejando as possibilidades de obtenção dos resultados negociais pretendidos, com a situação fática e conjuntural do SEPINF, pode-se excluir a opção de empregar software público, livre ou gratuito, pois não há nos portais de referência na internet, produtos que atendam todas as funcionalidades previstas, mesmo que fossem agregadas várias soluções diferentes, registrando que essa hipótese resultaria também em diminuição da eficiência e aumento de prazo para realizar os exames periciais. Foi consultado o portal www.softwarepublico.gov.br, na área "Segurança e Ordem Pública", nos termos da Portaria STI/MP

nº 46, de 28 de setembro de 2016. Em relação a softwares livres e gratuitos, os que são possíveis de serem utilizados já são amplamente empregados nos trabalhos periciais, a exemplo de Autopsy, Caine, DEFT entre muitos outros. Registre-se que não há solução similar em outro órgão ou entidade da Administração Pública.

Vale dizer que outros softwares proprietários já estão em uso também, portanto, os principais fornecedores de solução em informática forense tem produtos utilizados no SEPINF e nas demais unidades de perícia em informática da Polícia Federal. Por fim, esclarece-se que no momento atual o esforço de desenvolvimento próprio já está comprometido, por conta de projetos estratégicos como IPED, Nudetective, Inteligeo entre outros, portanto, a execução direta, por servidores do quadro não é possível, considerando os planos já formulados. De toda sorte, a solução pretendida envolve software específico, logo, escapa às atribuições do SEPINF em se aplicar numa atividade própria da iniciativa privada. Ressalta-se que os custos altos e a incerteza de obter resultados é bem patente, bastando para tanto avaliar o prejuízo na realização da Justiça, por não se lançar mão de produtos e serviços prontos e acabados, disponíveis no mercado.

A renovação dessas ferramentas é necessária para a manutenção da capacidade de realização de exames periciais em mídias de armazenamento computacional. Embora as licenças que já se encontram fora do período contratado de atualização sejam do tipo perpétuo, isto é, podem continuar a ser utilizadas, a falta de atualização as deixa defasadas em relação aos avanços tecnológicos e ao suporte de novas versões de sistemas operacionais, formatos de arquivos e artefatos digitais.

3.2. Objetivo da Contratação:

O objetivo da contratação é manter e ampliar a capacidade de análise em mídias de armazenamento computacional do Instituto Nacional de Criminalística e dos Setores, Unidades e Núcleos Técnicos-Científicos em todo o território nacional.

Visando atingir esse objetivo, os requisitos mínimos do equipamento a ser adquirido são:

- a) Forensic Toolkit (FTK): Atualizar 15 licenças já existentes do software AccessData Forensic Toolkit no formato de licença perpétua, com 03 anos de atualização e licenças concentradas em um servidor de licenças.
- b) IEF/Axiom: Atualizar com *trade-in* 100 licenças já existentes do Magnet Forensics IEF, convertendo-as para o Magnet Forensics Axiom Computer, com 03 anos de atualização.

3.3. Natureza da Contratação:

A contratação se dará pela modalidade inexigibilidade de licitação, pois cada um dos softwares contemplados possui um fornecedor exclusivo no Brasil (16645576 e 16645590). Verifica-se então, que há impossibilidade de competição, tanto pela exclusividade do objeto a ser contratado, como pela falta de empresas concorrentes.

3.4. Duração Inicial do Contrato:

A contratação da renovação deverá contemplar a entrega do produto em, no máximo, 90 dias após a assinatura do contrato e ainda vínculo de suporte e atualização por 36 meses após a entrega.

3.5. Sustentabilidade:

A empresa contratada deverá fornecer seus serviços em conformidade com normas e procedimentos técnicos e de qualidade, segurança, higiene, saúde e preservação ambiental. As políticas, os modelos e os padrões de governo não se aplicam diretamente à presente contratação, mas serão observados caso ocorra fatos que assim o justifiquem.

3.6. Relevância dos requisitos estipulados:

Os requisitos listados acima são, como já mencionados, essenciais para alcance dos objetivos propostos. No caso, o principal objetivo é manter a capacidade de realização de análises periciais em material apreendido de informática, imprescindível para atender a demanda dos Órgãos Centrais e Superintendências Regionais.

4. Estimativa das Quantidades:

a) Forensic Toolkit (FTK): Atualmente a Criminalística Federal dispõe de 180 licenças do software, expiradas em dezembro de 2018. Tendo em vista tratar-se de ferramenta complementar ao software IPED, utilizado como padrão de fato na Criminalística Federal e desenvolvido internamente, serão necessárias **15 licenças**, concentradas em um servidor de licenças mantido pelo SEPINF. Deste modo as licenças podem ser alocadas dinamicamente para utilização dos Peritos Criminais Federais da área de Informática em âmbito nacional.

b) IEF/Axiom: Atualmente a Criminalística Federal dispõe de 180 licenças do software IEF, atualmente descontinuado pelo fabricante (16627619) e com renovação comercializada apenas na modalidade

de *trade-in* para o seu sucessor, Magnet Forensics Axiom Computer. Tendo em vista a demanda de análises que necessitam de recursos oferecidos pelo Axiom Computer e que não estão disponíveis na ferramenta IPED, estimou-se um quantitativo de **100 licenças** para atender os 220 peritos em Informática em atividade, mais os atualmente em formação na Academia Nacional de Polícia, lotados em 46 unidades da Criminalística em todo o país.

5. Levantamento de Mercado e Justificativa da Escolha do Tipo de Solução a Contratar:

5.1 Identificação das soluções:

Conforme já mencionado, as soluções técnica e economicamente viáveis estão fora do campo de desenvolvimento por execução direta, bem como por software público, livre ou gratuito. Portanto, resta renovar as licenças dos softwares já utilizados, pois fazem parte do arcabouço de soluções que atendem ao SEPINF atualmente.

O mercado de soluções na área de informática forense é restrito, do ponto de vista da oferta de vários produtos, para atender a mesma necessidade de negócio. Atualmente há por volta de cinco fabricantes que tem mantido soluções longevas. De outro lado, a estratégia de comercialização desses produtos, porque limitada a quantidade de clientes, também é bem estrita. Veja-se que no Brasil há por volta de vinte e oito órgãos periciais que são potenciais adquirentes de soluções dessa natureza, considerando as vinte e sete Unidades da Federação e a Polícia Federal que tem representações em todo território nacional.

5.2 Análise comparativa das soluções

Os principais fornecedores são Access Data, Cellebrite DI, Guidance Software Inc, Magnet Forensics Inc. e Belkasoft, podendo acrescentar-se BlackBag Technologies Inc, uma subsidiária da Cellebrite, e a Nuix Pty Ltd, que concorre com produtos mais focados na análise de grandes volumes de dados com visualização gráfica. Oxygen Forensic e MSAB (Micro Systemation) possuem soluções menores que não fazem da parte da presente proposta de solução, podendo ser alvo de futura aquisição. Teel Technologies oferece soluções próprias e de terceiros, porém, sem contato no Brasil

Apesar das empresas serem de tecnologia, o modelo de negócio é bem tradicional, como se vê nos respectivos portais de internet. Portanto, no presente momento, a melhor solução é renovar as licenças dos softwares existentes, que são parte central na atividade de exames periciais e seguir avaliando outras ferramentas que podem complementar a solução existente, porque nenhuma das empresas acima oferecem solução única que atenda a todos os requisitos de negócio que serão apresentados no Capítulo 7. Descrição da Solução. Ou seja, essas ferramentas são fundamentais e não há substitutos até a presente data.

6. Estimativas de Preços ou Preços Referenciais:

A expectativa do custo do item é proveniente da cotação elaborada pelo fornecedor exclusivo (Techbiz) e do estudo de propostas recentes e minimamente similares oferecidas pelo mesmo a outros clientes. Por se tratar de software especializado com demanda pequena no Brasil, não foi possível encontrar aquisições semelhantes realizadas no ano de 2020 e, no caso do FTK, foram localizadas apenas duas comprovações. Ressalte-se que se trata de produto importado, de modo que na comparação de valores deve-se considerar a cotação do Dólar Norte-Americano (USD).

Proposta Techbiz:

Renovação IEF/Axiom	3.731.994,00
Renovação FTK	464.914,35

Total: R\$ 4.196.908,35

Comparativo com aquisições semelhantes:

Renovação IEF/Axiom:

Órgão/Empresa	OBJETO	Valor Total	Valor Unitário (Valor anual)	Dólar Mês	Valor Corrigido (Dólar = R\$ 5,20)	Valor Ajustado para 100 unidades e 3
---------------	--------	-------------	------------------------------	-----------	------------------------------------	--------------------------------------

Contratante		(R\$)	(R\$)	Contrato	(R\$)	anos (R\$)
NF 1292/2019 CENTRALSEG	Axiom módulo Computer (01 licença/01 ano)	17.065,64	17.065,64	4,0601	21.856,93	6.557.079,50
Contrato 877/2018 SSP PR 21/11/2018	Atualização e Trade in do IEF para Axiom por 12 meses (15 licenças)	185.440,95	12.362,73	3,7866	16.977,28	5.093.184,00
Contrato 122/2019 MP MG 27/08/2019	Atualização e Trade in do IEF para Axiom por 24 meses (01 licença)	33.865,73	16.932,87	4,158	21.176,26	6.352.878,00
Proposta Techbiz	Atualização e Trade in do IEF para Axiom Computer por 36 meses (100 licenças)	3.731.994,00	12.439,98	5,20	12.439,98	3.731.994,00

Renovação FTK:

Orgão/Empresa Contratante	OBJETO	Valor Total (R\$)	Valor Unitário (Valor anual) (R\$)	Dólar Mês Contrato	Valor Corrigido (Dólar = R\$ 5,20) (R\$)	Valor Ajustado para 10 unidades e 3 anos (R\$)
Contrato 235/2018 Min. Público MG	FTK Standalone com Belkasoft (01 licença/02 anos)	55.528,14	27.764,07	3,9330	36.708,15	1.651.866,86
NF 1106/2019 Min. Público SP	FTK Standalone (03 licenças/01 ano)	36.563,21	12.187,74	3,9650	15.983,92	719.276,26
Proposta Techbiz	FTK Standalone (15 licenças/3 anos)	464.914,35	10.331,43	5,20	10.331,43	464.914,35

7. Descrição da Solução como um todo:

A fim de se alcançar o objetivo pretendido, a solução como um todo abrange os seguintes produtos e especificações:

a) Forensic Toolkit (FTK):

- Licenças de uso de softwares de perícia forense em suite integrada ou não, na modalidade perpétua, com fornecimento de mídia de instalação em CD/DVD ou download direto do fabricante, próprio para realização de Perícia Forense e execução em Estação de Trabalho Local (Fixa ou Móvel), arquitetura Intel ou AMD, Sistema Operacional Windows 10;
- Deverá ter a capacidade de manipulação de dados através do uso de bases de dados de forma a garantir a flexibilidade, integridade e segurança dos dados armazenados;
- A solução deve suportar a execução dos serviços no sistema operacional Windows 10;
- Deve permitir a categorização automática de arquivos, diferenciando automaticamente

- grupos de informações, por status, extensões e tipo;
- Deve possuir tecnologia de quebra de senhas (abertura de criptografia) de dados com suporte a mais de 100 tipos de formato/dados;
 - Deve ter suporte a Unicode e a diferentes páginas de códigos;
 - Deve ser capaz de realizar o processamento e análise de e-mail com abertura automática de mensagens e anexos com suporte para os formatos: thunderbird, EML, Outlook Express DBX, Exchange EDB, Notes NSF, Outlook PST/OST e RFC 833;
 - Mecanismo avançado de data carving (extração de dados apagados) que deve procurar por critérios específicos, tais com o tamanho do arquivo, o tipo de dados e o tamanho dos pixels de forma a reduzir a quantidade de dados irrelevantes a serem buscados;
 - Deve ter mecanismo de relatórios, baseado em um assistente eletrônico que possibilite a exportação de relatórios detalhados nos formatos: PDF, HTML, RTF e XML;
 - Deve possuir módulo de reconhecimento de caracteres (OCR) que seja capaz de indexar e pesquisar caracteres encontrados em arquivos gráficos, como imagens e PDF;
 - Deve possuir um módulo de análise de arquivos maliciosos capaz de realizar de engenharia reversa automatizada determinando o comportamento e a intencionalidade de binários suspeitos;
 - Deve possuir a capacidade de visualização que exiba dados em linhas do tempo;
 - A solução deve possuir funcionalidades de marcação de documentos ou de parte de arquivos baseados em categorias definidas pelo usuário;
 - A solução deve possuir a capacidade de busca de variações gramaticais com expressões regulares por decorrência (stremming) ou proximidade;
 - A solução deve ser capaz de tratar arquivos Windows e de outros sistemas operacionais como Linux e MacOS, arquivos corrompidos, arquivos deletados, arquivos acima de 2Gb, e-mails e arquivos em uso e arquivos compostos (zip, rar, thumbs.db, email);
 - Deve ter a capacidade de realizar a leitura de imagens de disco tipo E01, SnapBack 2.0, Linux DD, ICS Ghost (somente a imagem forense), SMART e DMG;
 - Permitir a capacidade de criar e exportar listas de hash MD5, SHA1 e SHA256 de discos e arquivos em extensão "cvs";
 - Disponibilizar um conjunto de ferramentas que contemplam recuperação de senhas, geração de imagens de discos, visualização e interpretação de registros do Windows;
 - Fornecer o Suporte a imagens em CD e DVD das seguintes aplicações: Alcohol (*.mds), CloneCD (*.ccd), ISO, IsoBuster CUE, Nero (*.ccd), Pinnacle (*.pdi), PlexTools (*.pxi), Roxio (*.cif) e Virtual CD (*.vc4);
 - Possuir a capacidade de recuperar senhas EFS, em Windows 10;
 - Possuir a capacidade de criar imagens de disco em formato E01, AFF, Smart e RAW;
 - Possuir a capacidade de indexar o conteúdo dos arquivos de evidências;
 - Deve suportar os seguintes sistemas de arquivo: FAT12, FAT16, FAT32, NTFS, EXT2/3/4, exFAT, VxFS, ReiserFS 3;
 - Permitir a visualização de vários arquivos já pré-organizados por extensão pela ferramenta, de forma nativa;
 - Permitir a visualização de mensagens de correio eletrônico (emails) encontrados de forma nativa;
 - Permitir a visualização de arquivos gráficos (figuras, fotos, etc) de forma nativa;
 - Efetuar análise de assinaturas e extensões de arquivos, evidenciando se os mesmos foram renomeados propositalmente;
 - Realizar filtros pré-definidos na aplicação e possível de customização via script;
 - Permitir a criação de indexes com objetivo de aperfeiçoar as habilidades de busca;
 - Possibilitar a geração automática de relatórios a partir de marcações feitas durante a investigação;
 - Possuir recurso para recuperação de senhas que suportem os formatos de arquivos gerados pelos seguintes aplicativos: ABI Coder; MS Access; ACT; AIM; AmiPro; AOL; Approach; ARJ; Ascend; Ashampoo; BestCrypt; BPFTP; CDLock; CheckWriter; CodedDrag; crypt; Cryptainer; CryptaXix; Cryptext; CuteFTP; DataPerfect; dBASE; DriveCrypt; DriveCryptPP; EasyCrypto; EFS;EMF; FileMaker; Hello; ICQ; InvisibleSecrets; Justsystem; Kaikei; KeePass; Kremlin; Lockit; Lotus123; MaxCrypt; MessengerPlus; Money; MozillaMasterPassword; MozillaProtectedData; MSBackup; MSMail; MSNMessenger; MYOB; NetscapeMail; Microsoft Office; Omziff; OpenOffice; Organizer; Palm; Paradox; PasswordPal; PasswordSafe; PCEncrypt; PDF; PFX; PGP; PGPDisk; ProtectedRegistry; ProWrite; PST; PWL; QuattroPro; Quickbooks; Quicken; RARPassword; SafeHouse; SAMFile; Scheduler; ScreenSaver; SecretStuff; SecureIT; SiFEU; SourceSafe; Steganos; STools; SymantecQA; TrueCrypt; VBA; VersaCheck; Whisper; WinZip9; WordPerfect; WordPro; WS_FTP; XPCredentials; YahooMessenger; ZIP;
 - Possuir recurso para ataque de força bruta a senhas que usa processamento distribuído, utilizando o tempo ocioso das CPU's para auxílio na quebra de senha;
 - Possuir a capacidade de executar buscas por strings em memória, com mapeamento das strings encontradas com o respectivo processo ou mesmo DLL;
 - Possuir capacidade de análise de sistema operacional Apple, com suporte a arquivos JSON, database SQLite, PLIST, atributos B-Trees e imagens de discos padrão DMG;
 - Deverá possuir a capacidade de calcular *hashes* de arquivos e imagens;
 - O software deve obrigatoriamente ter licença de utilização perpétua;
 - A empresa deve fornecer atualização para novas versões por no mínimo 03 (três) anos.

b) IEF (trade-in para Axiom):

1. Características gerais da solução (Módulo Computer):

- a. Possuir suporte à aquisição de dispositivos móveis, discos, dispositivos USB, pastas arquivos e máquinas;
- b. Permitir aquisição de dispositivos móveis com sistema operacional Android, e iOS;
- c. Permitir aquisição de sistemas operacionais Windows, OS X, Linux;
- d. Permitir gerar relatórios nos formatos XML, HTML, PDF, CSV, Portable Case, Projeto CAID e Project VIC;
- e. Permitir o cálculo de HASH MD5 e SHA-1;
- f. Permitir realizar pesquisas utilizando REGEX e GREP;
- g. Permitir realizar a extração e análise dos dados utilizando uma única plataforma;
- h. Permitir aplicação de filtros para agilizar a pesquisa por artefatos;
- i. Permitir realizar a marcação de arquivos por meio de tags;
- j. Permitir gerar visualização utilizando Timeline;
- k. Permitir visualizar dados que possuem dados geográficos no mapa (geolocalização);
- l. Permitir realizar uma pré-visualização dos arquivos analisados em uma mesma interface;
- m. Permitir visualizar os arquivos no formato Hexadecimal para uma análise mais profunda dos dados;
- n. Permitir a exportação dos dados encontrados no arquivo de evidência;
- o. Permitir realizar comparação entre casos analisados;
- p. Permitir a recuperação de arquivos deletados e não sobrescritos;
- q. Permitir colaboração e compartilhamento de evidências;
- r. Permitir recuperar o Backups do iTunes para iOS 10.x:
 - i. Permitir analisar os e-mails contidos em OST, do Outlook 2013 e Outlook 2016.
- s. Permitir recuperar informações de quando um arquivo de torrent foi criado, modificado e baixado;
- t. Permitir busca por palavra chave em sistema de arquivos;
- u. Permitir analisar artefatos P2P em dispositivos Android:
 - i. Search BitTorrent;
 - ii. tTorrent Lite;
 - iii. uTorrent;
 - iv. Frostwire;
 - v. aTorrent;
 - vi. aDownloader.
- v. Permitir recuperar mais de 21 formatos de imagem RAW;
- w. Permitir verificação baseada em Hash de imagem forense E01;
- x. Possuir interface em no mínimo Inglês e Português – Brasileiro;
- y. Permitir a inserção da chave de criptografia de um disco criptografado com BitLocker antes do processamento do mesmo;
- z. Possuir integração com Passware;
- a. Permitir a criação de perfis de artefatos para diferentes tipos de casos;
- ab. Permitir a utilização de senhas conhecidas para descriptografar um disco criptografado pelo McAfee;
- bc. Possuir a capacidade de realizar o correlacionamento dos dados.

2. Tipos de dados mínimos suportados (computadores):

- a. Gmail, GMX, Hotmail, Hushmail, Mailinator, MBOX, Outlook.com, Yahoo!.
- b. Redes sociais Bebo, Facebook, Google+, Instagram, LINE, LinkedIn, MySpace, Twitter, Sina Weibo, VK;
- c. Bate papos Adium, AIM, Chatroulette, GoogleTalk, iChat, iMessage, Mail.ru, MSN Messenger, MSN Plus!, ICQ, Mail.ru, mIRC, Omegle, ooVoo, Paltalk, Pidgin, QQ Chat, Second Life, Skype, TorChat, Trillian, WeChat, Windows Live Messenger, World of Warcraft, Viber, Yahoo Messenger;
- d. Navegadores 360 Browser, Chrome, Edge, Internet Explorer, Firefox, Opera, Safari, Xbox IE;
- e. Dados de navegação refinados;
 - i. URLs e-commerce, Cloud Service URLs, Facebook URLs, Google Analytics Cookies, Google Maps Queries, Identifiers, Malware/Phishing URLs, Parsed Search Queries, Pornography URLs, Rebuilt Webpages, URLs de redes sociais;
- f. Aplicações de compartilhamento de arquivos, Bitcoin, eMule, Frostwire, Gigatribe, Limerunner, Limewire, Luckywire, Shareaza, .torrent files, Usenet
- g. Cloud services;
 - i. Carbonite, Dropbox (including Dropbox database decryption), Google docs, Google Drive, Flickr, Sharepoint, SkyDrive/OneDrive.
- h. Fotos e vídeos (EXIF data)

- i. 3GP, AMR, AVI, BMP, DIVX, GIF, ICO, JPEG, JPG, MP4, MKV, MOV, MPEG, MPG, PNG, TIF, TIFF, WMP.
- ii. Web video recovery Adobe Flash, Chatroulette, Camstumble, ChatForFree, iCU2, Shockrooms, YapChat;
- i. Mobile backups Android backups, iOS backups, Itunes;
- j. Arquivos Binreader, Grabit, NewzToolz-EZ, Newsbin, Forte Agent, Xnews.
- k. Bing Maps, Google Maps;
- l. Bing Toolbar, Google Toolbar;
- m. E-mails e mensagens mbox email archives, Microsoft Lync/OCS IM, Outlook OST & PST files, ZOOM;
- n. Document file artifacts .doc & .docx, .xls & .xlsx, .pdf, .ppt & .pptx;
- o. Logs de eventos, Jumplist, LNK files, Mounted network shares, OS and file system info, Prefetch files, Shellbags, Startup items, Time zones, User accounts, USB devices;
- p. Sistema de arquivos: NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, YAFFS2, APFS;
- q. Partições, volumes, arquivos e pastas, imagens, JTAG and chip-off imagens, compartilhamento de redes, captura de RAM, Imagens lógicas e físicas de dispositivos móveis, volume shadow copies;
- r. Imagens forenses – formatos de arquivo: E01, Ex01, L01, Lx01, AD1, dd, raw, bin, img, dmg, flp, vfd, bif, vmdk, vhd, vdi, xva, zip, tar;
- s. Pagefile.sys, \$MFT, \$Logfile, files and folders, hiberfil.sys, unallocated clusters, unpartitioned space, file slack space, swap file;
- t. Detecção automática de criptografia Truecrypt, Bitlocker, PGP, and Safeboot;
- u. Capacidade de pré-visualização de arquivos plist;
- v. Capacidade de pesquisa em imagens não encriptadas de dispositivos T2;
- w. Capacidade de pesquisa do espaço não alocado em uma imagem APFS;
- x. Suporte de análise para itens recuperados de \$RECYCLE.BIN.

3. Características mínimas de inteligência:

- a. Permitir categorização de dados automática;
- b. Identificar palavras-chave em plataformas de busca;
- c. Remontar páginas da Web em sua forma original;
- d. Remontar mapas, imagens e coordenadas do Google Maps;
- e. Possuir capacidade de identificar imagens de nudismo através de tons de pele;
- f. Detectar partes do corpo;
- g. Realizar pesquisas padrões de cartões de credito, endereços de e-mail e números de telefone;
- h. Possuir capacidade de reconstruir fragmentos de páginas de internet;
- i. Ter a capacidade de efetuar busca por artefatos de internet em extração lógicas ou físicas (dump de memória) de sistemas operacionais iOS e Android;
- j. Possuir suporte para artefatos OnStar RemoteLink;
- k. Possuir suporte para artefatos ninho no iOS, incluindo horários termostato, as configurações de usuário e configurações de localização;
- l. Possuir suporte para Fitbit;
- m. Possuir suporte para recuperação dos dados a partir do aplicativo Amazon Alexa em ambos Android e iOS;
- n. Possuir a capacidade de distinguir entre o formato .raw forense e o formato .raw utilizado em imagens;
- o. Possuir suporte a Nest, Amazon Echo, Fitbit e OnStar;
- p. Permitir a exportações do Project VIC contendo o ID da fonte possibilitando identificar a fonte de origem da imagem ou o vídeo.

4. Características mínimas de manutenção e software:

- a. A manutenção inclui direito a receber novas atualizações e correções do software através de correio eletrônico, contendo link para baixá-las, por 03 anos.

8. Justificativas para o Parcelamento ou não da Solução:

A existência de um único fornecedor com exclusividade comprovada, por si já demonstra a inviabilidade de parcelar a solução, posto que cada um dos produtos software é monolítico entre fornecedores, ou seja, não funcionam de modo integrado. O parcelamento da solução só faria sentido se fosse técnica e economicamente viáveis, porém, tecnicamente a impossibilidade é absoluta, porque cada fornecedor decide que porção da informática forense empreenderá esforços para desenvolver solução comercial. Portanto, a

renovação das licenças dos itens apresentados como solução, representa solução estanque, para cada uma delas. Por certo que o produto de cada uma é utilizada em várias fases do processo do exame pericial, mas não é possível separar cada licenciamento em parcelas distintas.

Vale dizer que a necessidade de manter uniforme a capacidade de análise das unidades técnico-científicas em todos os Estados do país e a economia de escala obtida por meio de compra centralizada, se beneficiará da impossibilidade de parcelamento intrínseca a cada solução. O fato é que cada um dos itens a serem contratados representam uma unidade ampla de funcionalidades, porém, acopladas de acordo com sistemática oferecida pelo fornecedor.

9. Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais ou financeiros disponíveis:

As licenças de software que se pretende renovar foram objeto de vultoso investimento da Administração ao longo dos últimos 5 anos e constituem ferramenta de uso diário dos Peritos Criminais Federais da área de Informática em sua tarefa de examinar mídias digitais e dispositivos móveis em busca de vestígios indicativos de materialidade e autoria de fatos delituosos. O corpo funcional encontra-se capacitado para a utilização dessas ferramentas, as quais se tornaram padrão de fato da área de Informática Forense da Polícia Federal. Tal padronização se mostrou benéfica na unificação dos procedimentos e processos, bem como na uniformização dos laudos periciais e na compatibilização das ferramentas internas de análise dos dados (IPED).

A presente renovação trará como benefícios a preservação dos recursos já investidos nas ferramentas e manutenção da capacidade de realização de exames da Criminalística Federal na área de Informática.

10. Providências para adequação do ambiente do órgão:

Não serão necessárias providências para adequação do ambiente, considerando que os laboratórios existentes atualmente suportam receber as aquisições, tanto na unidade central, quanto nas unidades descentralizadas.

11. Do Acesso às Informações contidas nos presentes Estudos Preliminares:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que as informações contidas nos presentes Estudos Preliminares **ASSUMEM CARÁTER PÚBLICO**.

12. Declaração de Viabilidade ou não da Contratação:

Considerando-se os elementos técnicos coligidos neste estudo preliminar, entende-se que as renovações por inexigibilidade dos softwares elencados constituem solução viável. E, ainda, a contratação é imperativa para o atendimento de demandas frequentes da criminalística como por exemplo a extração ágil de dados de mídias de armazenamento computacional para subsidiar investigações e ações de inteligência.

13. Responsabilidade da Equipe de Planejamento pela Elaboração e Conteúdo do Documento:

CERTIFICAMOS que somos responsáveis pela elaboração do presente documento que compila os Estudos Preliminares do Órgão Gerenciador e Participante(s) e que o mesmo traz os conteúdos previstos na Instrução Normativa nº 01/2019 - SEGES/ME.

ELCIO RICARDO DE CARVALHO
Matrícula DPF 9.250

APROVO o presente Estudo Técnico, tendo em vista que a presente contratação encontra-se alinhada ao Planejamento Estratégico da Polícia Federal, fazendo parte das atividades do SEPINF/INC/DITEC/PF para o atingimento das missões institucionais do órgão.

ROSEMEIRE ABADIA MOREIRA
Perita Criminal Federal
Chefe do SEPINF/DPER/INC/DITEC/PF



Documento assinado eletronicamente por **ROBEMAR BICALHO RODRIGUES, Agente Administrativo(a)**, em 10/11/2020, às 10:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **ELCIO RICARDO DE CARVALHO, Perito(a) Criminal Federal**, em 10/11/2020, às 10:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **ROSEMEIRE ABADIA MOREIRA, Chefe de Serviço**, em 10/11/2020, às 12:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **ALAN DE OLIVEIRA LOPES, Diretor(a)**, em 11/11/2020, às 12:05, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **16627209** e o código CRC **2B1C476A**.