DIRETORIA DE TECN.DA INFORMAÇÃO E INOVAÇÃO

Estudo Técnico Preliminar 19/2025

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

2.1. Necessidade de Sistema Automatizado de Identificação Biométrica (ABIS) para 277,6 milhões de pessoas.

2.2. Necessidade de Sistemas Clientes para Estação de Trabalho Pericial, Estação de Cadastramento e Dispositivos Móveis.

2.3. Necessidade de serviços para implantação, capacitação e manutenção do sistema.

2.4. Motivação e justificativas:

2.4.1. DFD de origem: 157/2025

2.4.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026.

2.4.3. O objeto da contratação também está alinhado com o Planejamento Estratégico da Polícia Federal 2024-2027, com o Planejamento Estratégico do Ministério da Justiça e Segurança Pública 2024-2027 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2024-2027 da Polícia Federal, conforme demonstrado abaixo:

Objetivos Estratégicos
Plano Tático-Operacional Orientado a Resultados-Chave PTO-KR/DPA/PF-2024/2025 Objetivo Estratégico 4: Formar a polícia do futuro, moderna e inovadora KR Tático-Operacionais 4.1.1.1: Ampliar para 250 milhões a capacidade de armazenamento de registros no sistema ABIS.
Planejamento Estratégico da Polícia Federal 2024-2027 conforme RESOLUÇÃO CG/PF Nº 007, DE 27 DE MAIO DE 2024 (art. 11, § 5º, inc. IV): Ampliação da base do ABIS - Solução Automatizada de Identificação Biométrica.
Planejamento Estratégico do Ministério da Justiça e Segurança Pública 2024-2027 Objetivo Estratégico 3: Fortalecer a prevenção e o enfrentamento à criminalidade. Código do Plano Interno 1K: Implementar uma solução de abrangência nacional, com o fim de estabelecer ações para viabilizar a unificação e a padronização das informações relativas às identificações civis e criminais dos órgãos de segurança pública dos Estados, do Distrito Federal e da Polícia Federal, possibilitando maior eficiência na identificação do cidadão, de modo a contribuir para a segurança de suas relações com o Governo e para o enriquecimento do corpo probatório, bem como para a redução do índice de criminalidade.

ALINHAMENTO AO PDTIC 2024-2027			
ID da Necessidade	Necessidade de TIC	ID da Ação de TIC	Ação de TIC
N6	Manutenção e modernização do parque tecnológico e da infraestrutura de TIC	A80	Contratar infraestrutura para expansão da solução ABIS
N7	Manutenção, aquisição, evolução e desenvolvimento de soluções de TIC	A165	Expansão da solução ABIS
N7	Manutenção, aquisição, evolução e desenvolvimento de soluções de TIC	A177	Contratar estação móvel offline de verificação biométrica

2.4.4. A contratação de um sistema ABIS (Sistema Automatizado de Identificação Biométrica) para a Polícia Federal justifica-se pela necessidade de adequação da capacidade do sistema atual, conforme exposto no DFD Digital 282/2024. A capacidade contratada de armazenamento e individualização do Sistema Biométrico administrado pela Polícia Federal, conforme Pregão Eletrônico n° 4/2020 - DTI/PF, foi de 50,2 milhões de Registros de Pessoas no comparador da solução e de 40 mil pesquisas biométricas diárias.

2.4.5. No entanto, a partir de acordos de cooperação técnica, convênios e outras integrações com as Secretarias de Segurança Pública, o MGI e outras instituições, a demanda de armazenamento e o processamento biométrico no sistema ABIS aumentou. No momento, já foram processadas e armazenadas 14.8 milhões de novas Pessoas no ABIS desde a implantação em novembro de 2022, totalizando 39 milhões de pessoas no comparador do ABIS. O INI possui mais de 20 milhões de novos registros biométricos aguardando inclusão, além das demandas internas de processamento e armazenamento de biometrias de Passaportes, de Registro Nacional Migratórios, de Carteiras de Segurança Privada e de coletas criminais, ultrapassando a capacidade contratada de 50,2 milhões.

2.4.6. Considerando o compartilhamento de dados previsto nos acordos de cooperação com as administrações estaduais das 27 Unidades da Federação, a capacidade de armazenamento necessária para o sistema ABIS administrado pela Polícia Federal será de 277,6 milhões de pessoas para todo o contrato.

2.4.7. Conforme previsão no Plano Estratégico da Polícia Federal 2024-2027, Resolução CG/PF nº 007, de 27 de maio de 2024, um dos objetivos estratégicos do eixo de pessoas e estrutura é a ampliação da base do ABIS – Solução Automatizada de Identificação Biométrica (art. 11, § 5º, inc. IV), que trata de uma ferramenta de auxílio ao enfrentamento eficiente da criminalidade (art. 11, § 1º, inc. I) e da prestação dos serviços a sociedade com transparência e excelência (art. 11, § 1º, inc. II).

2.4.8. Em alinhamento ao objetivo estratégico de consolidar a Polícia Federal como instituição orientada pela estratégia e pela governança (art. 11, § 1º, inc. III), a implantação de um banco biométrico nacional, capaz de absorver identificações provenientes de outras instituições, configura necessidade imediata. A adequação do ABIS permitirá à Polícia Federal, com sua atuação nacional nas esferas judiciária e administrativa, assumir papel central na identificação inequívoca do cidadão, tanto para fins civis quanto criminais.

2.4.9. Como competência da Segurança Pública, a identificação humana, tanto civil quanto criminal, configura atividade essencial à manutenção da ordem pública e à promoção da cidadania, estando sob responsabilidade desse setor desde o início do século XX no Brasil. Trata-se de atribuição exercida por servidores de carreira típica de Estado, legalmente investidos e especializados, que integram a estrutura da própria Segurança Pública.

2.4.10. No âmbito da identificação civil, o Decreto nº 11.797, de 27 de novembro de 2023, que dispõe sobre o Serviço de Identificação do Cidadão e sobre a governança da identificação das pessoas naturais no âmbito da administração pública

federal direta, autárquica e fundacional e institui a Câmara-Executiva Federal de Identificação do Cidadão – Cefic, determina que compete à Polícia Federal subsidiar técnica e operacionalmente os processos de identificação inequívoca da pessoa natural nos bancos de dados biométricos (art. 22, inc. III), bem como disponibilizar os subsídios procedimentais e técnicos necessários para o acesso à sua base biométrica, garantida a segurança técnica e jurídica das transações e fluxo de dados (art. 22, inc. IV) e apoiar tecnicamente os processos de auditoria e fiscalização dos sistemas biométricos utilizados na expedição da Carteira de Identidade (art. 22, inc. V).

2.4.11. Esse decreto também estabelece que o compartilhamento de dados pessoais entre órgãos e entidades da administração pública no âmbito do Serviço de Identificação do Cidadão observará a existência de finalidades legítimas, específicas e explícitas, além da compatibilidade entre o tratamento do dado com as finalidades (art. 7º, incs. I e II).

2.4.12. Desse modo, a Polícia Federal já está inserida de modo direto nas ações para identificação do cidadão, corroborando sua atribuição originária de coordenar e interligar no país, as identificações civis e criminais (Lei nº 4.483/64).

2.4.13. Considerando que a identificação inequívoca do cidadão requer a constituição de uma base central biométrica, administrada e operacionalizada por profissionais da carreira típica de Estado legalmente responsáveis pela atividade de identificação humana, a Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe que, em nenhuma hipótese, a totalidade dos dados pessoais destinados à Segurança Pública poderá ser tratada por entes privados, salvo se integralmente controlados pelo poder público (art. 4º, inc. III, § 4º). Nesse contexto, compete à Polícia Federal, instituição com atuação nacional, desenvolver e adequar suas ferramentas às diretrizes de seu Plano Estratégico, aos projetos de governo e às políticas públicas, assumindo protagonismo na governança de um banco nacional biométrico. Isso inclui a capacidade de absorver registros de identificação oriundos de outras instituições para fins de processamento, tratamento e individualização, assegurando o cumprimento de seu papel constitucional por meio de seus especialistas.

2.4.14. Sobre esse assunto, a Lei nº 13.444/2017, que dispõe sobre a Identificação Civil Nacional traz que ato do Tribunal Superior Eleitoral disporá sobre a integração dos registros biométricos pelas Polícias Federal e Civil, com exclusividade, às suas bases de dados (art. 3º, § 2º).

2.4.15. A análise dos registros biométricos é atribuição dos Institutos Oficiais de Identificação, institutos esses, que inclui o Instituto Nacional de Identificação da Polícia Federal, instituições com autonomia técnica, científica e funcional garantida pela Lei nº 13.675/2018, essa autonomia se refere à liberdade técnico-científica para a realização e a conclusão de procedimentos e exames inerentes ao exercício de suas competências, conforme Decreto nº 9.489/2018.

2.4.16. Sendo a identificação humana civil e criminal no âmbito da administração pública federal direta, competência do Instituto Nacional de Identificação da Polícia Federal, cabe a Polícia Federal adequar sua ferramenta para que seu serviço de identificação possa desenvolver os procedimentos e fluxos para o tratamento efetivo e eficaz dos dados sensíveis dos cidadãos que forem demandados à Polícia Federal, sejam eles com a finalidade civil ou criminal.

2.4.17. No âmbito da identificação criminal, a Lei nº 13.964/2019, que aperfeiçoou a legislação penal e processual penal autorizou a criação no âmbito do Ministério da Justiça e Segurança Pública de um banco nacional multibiométrico e de impressões digitais. E no âmbito do Ministério da Justiça e Segurança Pública, a Polícia Federal já possui um banco multibiométrico com abrangência nacional. Por essa Lei, está autorizado compor esse banco os registros provenientes da identificação criminal (§ 3º), da identificação prisional (§ 4º) e da identificação civil geridos por órgãos dos Poderes Executivo, Legislativo e Judiciário das esferas federal, estadual e distrital, inclusive pelo Tribunal Superior Eleitoral e pelos Institutos de Identificação Civil (§ 5º). E a integração ou a interoperação dos dados de registros multibiométricos constantes de outros bancos de dados com o Banco Nacional Multibiométrico e de Impressões Digitais ocorrerá por meio de acordo ou convênio com a unidade gestora (§ 7º).

2.4.18. Atualmente, existem Acordos de Cooperação Técnica entre a Polícia Federal e os órgãos de Segurança Pública das Unidades Federativas, que preveem a integração e a interoperabilidade interinstitucional, tendo a Polícia Federal um papel importante como órgão central de absorção dos registros de identificação e compartilhamento operacional do ABIS, o que tem tornado mais efetiva a atuação dos Institutos Oficiais de Identificação na prevenção e repressão aos crimes de falsidade ideológica e falsa identidade.

2.4.19. Desse modo, a atuação da Polícia Federal no âmbito da identificação humana está em uma posição privilegiada, em conformidade com as legislações e ao encontro das políticas públicas sobre identificação inequívoca do cidadão, justificando a presente intenção de compra.

3. Área requisitante

Área Requisitante	Responsável
INI/DPA/PF	Fernando Ferreira Rezende Freitas

4. Necessidades de Negócio

4.1. Atender aos requisitos funcionais de:

4.1.1. Pesquisas Biométricas

4.1.1.1. O Sistema deverá realizar pesquisas biométricas conforme a tabela:

	Impressão Digital	**Impressão Palmar**	**Face**
Pessoa x Pessoa (PER/PER)	TP/TP	PP/PP	FF/FF
Pessoa x Caso	TP/UL	PP/UP	FF/UF
Caso x Pessoa	LT/TP	LP/PP	UF/FF
Caso x Caso	LT/UL	LP/UP	UF/UF

4.1.1.2. Pesquisa PER/PER: essa pesquisa corresponde ao conjunto de pesquisas TP/TP, PP/PP e FF/FF realizadas no momento da inserção de registro no ABIS.

4.1.1.3. Pesquisa sem Inserção: o sistema deverá também possibilitar a inserção temporária da biometria pesquisada. Os dados pesquisados nesta funcionalidade não serão disponibilizados ao usuário do sistema ao final da pesquisa, ocorrendo apenas salvamento dos dados pesquisados por esta modalidade no Banco de Dados do sistema ABIS para garantir uma possibilidade de auditoria futura, caso se faça necessário. Este tipo de solução deverá estar disponível para inserções de impressões digitais, palmares e face em conjunto ou de forma isolada.

4.1.1.4. Pesquisa Fechada: o Sistema deverá disponibilizar uma verificação de identificador externo na qual o novo registro irá ser confrontado com a passagem anterior existente da pessoa no sistema. A pesquisa fechada será realizada com utilização de um identificador externo ao sistema (RNM, RF, RPF, RPE ou CPF). Nos casos de NO HIT em pesquisa fechada com identificadores externos, a Solução encaminhará o documento para o Controle de Qualidade de Identificador Externo. Nos casos de HIT o fluxo do sistema seguirá normalmente com a unificação das fichas de registro.

4.1.1.5. Pesquisa de Autenticação: semelhante a pesquisa fechada, a pesquisa de autenticação será realizada com um identificador externo e quatro opções diferentes de inserção biométrica (dedo, 2 dedos, face, face e dedo).

4.1.1.6. Pesquisa Restrita: deverá ser possível realizar pesquisas contra uma lista de Registros de Pessoas ou de Casos.

4.1.2. Capacidade do Sistema

4.1.2.1. A nova Solução ABIS deverá permitir a operação dos atuais 40 milhões de Registros de Pessoas da solução em operação e de mais 237.6 milhões de Registros de Pessoas, totalizando 277.6 milhões de Registros de Pessoas nos comparadores biométricos da Solução, independentemente do número de Registro de Passagem de cada Pessoa.

4.1.2.2. Atualmente os 40 milhões de Registros de Pessoas correspondem a 46 milhões de Registro de Passagem. Mantida a proporção, a quantidade total de Registro de Passagem deverá ser de aproximadamente 319.2 milhões.

4.1.2.3. Cada Registro de Pessoa ou de Passagem poderá ser composto por:

4.1.2.3.1. até 10 impressões digitais roladas;

4.1.2.3.2. impressões digitais pousadas (para controle de sequência ou comparação);

4.1.2.3.3. impressões palmares (regiões interdigital, tenar e hipotenar) de ambas as mãos;

4.1.2.3.4. até 3 fotografias de face (fotografias frontal, lateral ou de perfil);

4.1.2.3.5. até 3 fotografias de tatuagem; e

4.1.2.3.6. dados identificativos.

4.1.2.4. O Sistema, no mínimo, deverá permitir:

4.1.2.4.1. comparação e o armazenamento de 319.2 milhões de decadactilares;

4.1.2.4.2. comparação e o armazenamento de 50 mil palmas de ambas as mãos;

4.1.2.4.3. comparação e o armazenamento de 319.2 milhões de fotografias de face frontal;

4.1.2.4.4. comparação e o armazenamento de 1.6 milhão de casos periciais de impressão digital;

4.1.2.4.5. comparação e o armazenamento de 40 mil casos periciais de impressão palmar;

4.1.2.4.6. comparação e armazenamento de 1 milhão de casos periciais de face.

4.1.3. Processamento de Transações

4.1.3.1. Pesquisas de autenticação (dedo, 2 dedos, face, face e dedo): 400 mil por dia;

4.1.3.2. Pesquisas PER/PER: 126 mil por dia;

4.1.3.3. Pesquisas TP/UL: 5000 por dia;

4.1.3.4. Pesquisas LT/TP: 350 por dia;

4.1.3.5. Pesquisas LT/UL: 350 por dia;

4.1.3.6. Pesquisas PP/PP: 50 por dia;

4.1.3.7. Pesquisas LP/PP: 50 por dia;

4.1.3.8. Pesquisas PP/ULP: 50 por dia;

4.1.3.9. Pesquisas ULP/ULP: 50 por dia;

4.1.3.10. Pesquisas UFACE/FACE: 3000 por dia;

4.1.3.11. Pesquisas FACE/UFACE: 3000 por dia;

4.1.3.12. Pesquisas UFACE/UFACE: 3000 por dia;

4.1.4. Tempos de resposta

4.1.4.1. Pesquisas de autenticação (dedo, 2 dedos, face, face e dedo): 1.5 segundos;

4.1.4.2. Pesquisas PESSOA/PESSOA (TP/TP e FACE/FACE): 30 segundos;

4.1.4.3. Pesquisas TP/UL: 3 minutos;

4.1.4.4. Pesquisas LT/TP: 10 minutos;

4.1.4.5. Pesquisas LT/UL: 3 minutos;

4.1.4.6. Pesquisas PP/PP: 3 minutos;

4.1.4.7. Pesquisas LP/PP: 3 minutos;

4.1.4.8. Pesquisas PP/ULP: 3 minutos;

4.1.4.9. Pesquisas ULP/ULP: 3 minutos;

4.1.4.10. Pesquisas UFACE/FACE: 3 minutos;

4.1.4.11. Pesquisas FACE/UFACE: 3 minutos;

4.1.4.12. Pesquisas UFACE/UFACE: 3 minutos;

4.1.5. Acurácia do sistema

4.1.5.1. A empresa deverá ter participado de testes OnGoing conduzidos pelo NIST (National Institute Of Standards and Technology), especificamente nos programas ELFT (Evaluation Of Latent Friction Ridge Technology) e FRTE (Face Recognition Technology Evaluation), conforme aplicável às modalidades de biometria digital e facial, respectivamente e cumulativamente.

4.1.5.2. A empresa terá que declarar que a solução proposta se relaciona aos softwares submetidos aos testes ELFT e FRTE.

4.1.5.3. Critério para impressões digitais latentes

4.1.5.3.1. Para avaliação do desempenho em comparação de impressões digitais latentes, será utilizado como referência o parâmetro rank-1 hit rate, no conjunto “FBI-Provided Solved Dataset #1”, para “probes with EFS data” (256 latentes) e “Proble Content” igual a “Image + EFS”, num banco de 1.600.000 impressões (N=1.600.000), constante na edição mais recente do teste ELFT vigente até a elaboração deste documento.

4.1.5.3.2. Será considerado como valor mínimo de qualificação o resultado de 93,7%. A medição de desempenho será baseada no resultado do teste mais recente do ELFT disponível até a elaboração deste documento.

4.1.5.4. Critério para reconhecimento facial

4.1.5.4.1. Para aferição de desempenho dos algoritmos de reconhecimento facial, será considerado o cenário Rank-1 (identification), VISA-BORDER, com um banco de dados de 1.600.000 faces (N = 1.600.000), com 1.212.892 imagens de 577.444 pessoas únicas.

4.1.5.4.2. Será considerado como critério mínimo de qualificação o valor de acurácia de 99,76%. A medição de desempenho será baseada no resultado do teste mais recente do FRTE disponível até a elaboração deste documento.

4.1.6. Funcionalidades do Sistema

4.1.6.1. Serviço de Consulta de Dados Identificativos: A consulta ao banco de dados deverá ser realizada por meio de um ou vários filtros, cada filtro correspondendo a um campo identificativo. O motor de busca de dados identificativos deverá contemplar a funcionalidade fonética, filtros por intervalos para os campos de data, aderência a caracteres curinga e tempo de resposta inferior a 10 segundos.

4.1.6.2. Controle de Qualidade Biométrico: o sistema deverá disponibilizar serviço de controle de qualidade manual de acordo com os limiares de qualidade parametrizados em ferramentas de administração com controle de qualidade e de quantidade das minúcias, controle e correção da sequência dos dedos (quanto disponíveis as impressões digitais pousadas), detecção de arrastamento de dedos e de sobreposição do efeito “cortina” e possibilidade de rejeição do registro pelo usuário com caixa de texto para justificativa da rejeição.

4.1.6.3. Controle de Qualidade de Identificador Externo: o sistema deverá disponibilizar um controle de qualidade para o identificador nos casos de NO HIT em pesquisas fechadas (1:1), através do qual a Solução encaminhará o documento para que o usuário possa modificar o identificador de um dos registros.

4.1.6.4. Inserção de Registro: o procedimento geral de inserção de Registros de Pessoa na base de dados permanente do ABIS deverá, no mínimo, realizar codificação e controle de qualidade, se necessário, Pesquisa Fechada (se houver identificador externo), pesquisa PER/PER, decisão automática de HIT ou NO HIT (lights-out) ou, ainda, por verificação manual nos casos necessários e criação de uma nova Pessoa no caso de uma decisão NO HIT.

4.1.6.5. ACE-V: todos os resultados de pesquisa com decisão realizada por operador poderão ser verificados, de acordo com a metodologia ACE-V. Desta forma, um confronto realizado por um usuário poderá ser apresentado para um segundo usuário da mesma agência que realizará nova decisão. Caso os dois usuários tenham avaliações diferentes sobre o confronto, o sistema deve disponibilizar o confronto para um terceiro usuário, que tomará a decisão final.

4.1.6.6. Lights-out: decisões de HIT ou NO HIT automáticas deverão ser tomadas de acordo com o placar, baseado no limiar de HIT e no limiar de NO HIT parametrizados em ferramenta de administração. Em caso de pesquisa PESSOA x PESSOA, serão levados em consideração os identificativos.

4.1.6.7. Matching Any Finger: deverá ser realizada a pesquisa biométrica de todos os dedos, de modo que um dedo possa ser localizado independentemente de sua posição.

4.1.6.8. Aquisição de Faces: o sistema deverá permitir a aquisição de imagens faciais a partir de diversas fontes, entre elas, a captura de faces visíveis em frames de vídeos e em imagens estáticas nos mais diversos formatos, além de apresentar a funcionalidade de processamento automático nas etapas de captura de imagens de faces contidas em frames de vídeos ou em imagens estáticas;

4.1.7. Funcionalidades de Administração

4.1.7.1. A Solução deverá disponibilizar funcionalidade e interface especializada para administração de rotinas e gestão do fluxo de trabalho.

4.1.7.2. O Sistema deverá contemplar funcionalidade e interface que permitam criação, edição e exclusão de contas de usuários, como também interface para controlar, monitorar e bloquear o acesso de usuários ao sistema.

4.1.7.3. O Sistema deverá contemplar funcionalidade e interface que permitam gerir as atribuições e perfis dos usuários. Atribuições são ações que a administração do sistema poderá habilitar ou desabilitar para os usuários. Perfis são conjuntos de atribuições definidos pela administração do sistema.

4.1.7.4. A Solução deverá contemplar funcionalidade e interface que permitam ao Administrador gerenciar os parâmetros que determinam quando o controle de qualidade manual é necessário tanto para as impressões digitais, impressões palmares e faces considerando: dedos com problema de sequência em seu posicionamento, número de dedos com uma pontuação mínima de qualidade insuficiente, número de dedos com um número mínimo de minúcias insuficiente, número de dedos não classificados, palmas com problemas de sequência, palmas com uma pontuação mínima de qualidade insuficiente, palmas com um número mínimo de minúcias insuficiente, faces com qualidade insuficiente.

4.1.7.5. O Sistema deverá contemplar funcionalidade e interface que permitam ao Administrador gerenciar, para pesquisas de pessoa e de casos, os parâmetros de: placar máximo de NO HIT, placar mínimo de HIT, aviso de verificação de NO HIT com placar alto e aviso de verificação de HIT com placar baixo.

4.1.7.6. Para cada procedimento de inserção no Sistema ABIS, a Solução deverá permitir a definição da agência que deverá executar as operações manuais (controle de qualidade e verificação), em função da origem da inserção no Sistema ABIS.

4.1.7.7. O Sistema deverá contemplar funcionalidade e interface que permitam ao Administrador avaliar a Solução por meio de ferramentas de monitoramento que reúnam e exibam automaticamente o status dos serviços do Sistema, contendo minimamente o devido funcionamento da comunicação entre servidores e sistemas clientes, do banco de dados, dos comparadores biométricos e das interfaces de APIs.

4.1.7.8. O Sistema deverá contemplar funcionalidade e interface que permitam ao Administrador que pare, inicie ou reinicie serviços de forma segura e simplificada, incluindo funcionalidade que permita ao Administrador o tratamento de serviços em estado de erro de forma segura e simplificada.

4.1.8. Réplica do banco de dados

4.1.8.1. A Solução deverá disponibilizar réplica do banco de dados de produção para realização de pesquisas e geração de relatórios pela CONTRATANTE. O banco réplica será utilizado para a elaboração de relatórios pela CONTRATANTE através de acesso direto por SGBD utilizado pela CONTRATANTE e deverá ser acessível e compatível com as ferramentas de Business Inteligence utilizadas pela CONTRATANTE.

4.1.8.2. O banco de dados réplica deve ser uma cópia atualizada do banco de dados de produção, com exceção dos campos que possuem dados biométricos. Nos campos do banco de dados de produção que contêm imagens de biometrias, estas deverão ser substituídas pelos seus respectivos HASH no banco réplica.

4.1.8.3. A replicação deve ser realizada de forma assíncrona e com frequência mínima de um dia para evitar impacto no desempenho do banco de dados de produção. O banco de dados réplica deverá ter uma disponibilidade igual ou superior ao banco de produção e deverá possuir mecanismos de backup e recuperação para garantir a disponibilidade dos dados em caso de falha.

4.2. Fornecer os Sistemas Clientes:

4.2.1. Os Sistemas Clientes ABIS são softwares que utilizam os serviços disponibilizados pelo Sistema ABIS Central e serão:

4.2.1.1. Software para Estação de Trabalho Pericial;

4.2.1.2. Software para Estação Cadastramento;

4.2.1.3. Aplicativo para Dispositivos Móveis de Identificação ou Autenticação Biométrica.

4.2.2. As licenças deverão ser de uso permanente, na modalidade flutuante.

4.2.3. Os Softwares para Estação de Trabalho Pericial e para Estação de Cadastramento deverão ser compatíveis com Windows 10 e superiores. Os computadores em que serão utilizados os sistemas clientes não serão de uso exclusivo dessas aplicações.

4.2.4. Deverá ser possível utilizar os Softwares para Estação de Trabalho Pericial e para Estação de Cadastramento no mesmo computador, sem incompatibilidades entre si.

4.2.5. O Aplicativo para Dispositivos Móveis de Identificação ou Autenticação Biométrica deverá ser compatível com sistemas Android (versão a ser definida) e IOS (versão a ser definida).

4.2.6. Os sistemas clientes deverão permitir login por meio do Active Directory (AD) da Polícia Federal, por meio de senha alfanumérica para usuários fora do AD e por meio da identificação biométrica do operador. O login por meio da identificação biométrica poderá ser desativado por decisão da Administração do Sistema.

4.2.7. Software para Estação de Trabalho Pericial

4.2.7.1. O software para Estação de Trabalho Pericial deverá operacionalizar os requisitos funcionais definidos no Item 4.1.

4.2.7.2. Funcionar de maneira assíncrona, ou seja, ter a capacidade de trabalhar off-line e sincronizar os dados coletados assim que houver conexão de rede. A base temporária, a ser sincronizada, dimensionada de acordo com a demanda, não deverá ter capacidade inferior a 1.000 cadastros.

4.2.8. Software para Estação de Cadastro

4.2.8.1. Software específico para coleta presencial de dados identificativos e biométricos, em estações de identificação no formato “kit portátil de identificação biométrica”, devendo ainda atender, minimamente, aos seguintes requisitos de software:

4.2.8.2. contemplar funcionalidade que permita inserir no ABIS uma Pessoa por captura das impressões digitais “*in vivo*”, com ou sem impressões palmares, monitoradas por controle de qualidade local, captura de fotografias de face, envio do registro ao Sistema ABIS, recepção da mensagem pelo Sistema ABIS, confirmação da recepção do registro cadastrado no ABIS e resultado de identificação de HIT ou NO HIT. Nesta modalidade de aquisição, caso

uma operação manual (controle de qualidade, verificação TP/TP) seja necessária, a agência que irá executá-la será definida em função da agência em que está cadastrada a Estação de Cadastramento;

4.2.8.3. contemplar recurso que permita realizar a autenticação de uma Pessoa de maneira rápida;

4.2.8.4. funcionar de maneira assíncrona, ou seja, a funcionalidade deverá ter a capacidade de trabalhar off-line e sincronizar os dados coletados assim que houver conexão com o Sistema ABIS Central. A base temporária deverá ter capacidade superior a 1.000 cadastros;

4.2.8.5. possibilitar a exportação da base local de aquisições para mídia externa (unidade de armazenamento conectada à porta USB da estação);

4.2.8.6. disponibilizar funcionalidades para o controle de qualidade da coleta e disponibilizar recursos que evitem fraudes com simulacros que se assemelhem à impressão digital;

4.2.8.7. permitir a visualização da imagem da impressão digital sendo capturada, em tempo real, na interface do usuário e possibilitar a visualização da impressão digital após a coleta;

4.2.9. Aplicativo para Dispositivos Móveis de Identificação ou Autenticação Biométrica

4.2.9.1. O Aplicativo para Dispositivos Móveis de Identificação ou Autenticação deverá ser capaz de realizar cadastramento, identificação e autenticação, online e offline. Os procedimentos poderão ser realizados capturando de uma a dez impressões digitais, fotografias de face ou as duas biometrias via Dispositivo, a critério do operador.

4.2.9.2. O Aplicativo deverá ser capaz de realizar a coleta das fotografias de face através da câmera fotográfica do Dispositivo ou importar imagem pré-existente na galeria do Dispositivo.

4.2.9.3. O Aplicativo deverá ser capaz de realizar a coleta de impressões digitais através de leitor biométrico conectado ao aparelho, através de câmera fotográfica do Dispositivo (funcionalidade “*contactless*”) ou importar imagem pré-existente na galeria do Dispositivo.

4.2.9.4. O Aplicativo para Dispositivos Móveis de Identificação ou Autenticação Biométrica deverá contemplar as seguintes características para Pesquisa Online:

4.2.9.4.1. funcionalidades para realizar pesquisa na base de dados central do ABIS com tempo de resposta inferior a 3 minutos para pesquisa, desconsiderando-se fatores externos como a disponibilidade da rede.

4.2.9.4.2. funcionalidades para realizar a autenticação e a identificação on-line, em que os Dispositivos se comuniquem diretamente com o Sistema ABIS Central;

4.2.9.4.3. funcionalidades para realizar o cadastramento de uma Pessoa online, mesmo que a internet não esteja disponível no momento da coleta. O registro deverá ser encaminhado para o Sistema Central do ABIS quando houver disponibilidade de internet.

4.2.9.4.4. a autenticação online utilizará os dados identificativos na base de dados central do ABIS como mecanismo de seleção de registro.

4.2.9.5. O Aplicativo para Dispositivos Móveis de Identificação ou Autenticação Biométrica deverá contemplar as seguintes características para a Pesquisa *Offline*:

4.2.9.5.1. funcionalidade para realizar pesquisa em uma base de dados local carregada no Dispositivo. A capacidade da lista local não deverá ser inferior a 200 mil registros. O tempo de resposta não poderá ser superior a 10 segundos para pesquisa na base de dados local;

4.2.9.5.2. funcionalidades para realizar a autenticação e a identificação *offline*, em que os Dispositivos utilizarão a Lista de Interesse local carregada no aparelho;

4.2.9.5.3. a autenticação *offline* utilizará os dados identificativos na base local com mecanismo de seleção de registro.

4.2.9.5.4. funcionalidades para realizar o cadastramento de uma Pessoa *offline*. O cadastramento *offline* deverá permitir salvar o registro em ZIP de imagens e dados identificativos, PDF, NIST ou JSON para inclusão posterior pelo operador.

4.2.9.6. O Aplicativo para Dispositivos Móveis de Identificação ou Autenticação deverá possuir funcionalidade de gerenciamento e administração, conforme acesso definido pela Administração do Sistema.

4.2.9.7. O Aplicativo deve registrar o histórico de autenticações, verificações e cadastramentos realizados, a quantidade de pesquisas realizadas, de cadastramentos e de hits, bem como de erros ocorridos. Deverá ser possível exportar relatório com essas informações.

4.2.9.8. Os dados identificativos e biométricos do histórico de autenticações, verificações e cadastramento poderão ser exportadas a qualquer momento, em formatos PDF, NIST ou JSON, a critério do operador. Em caso de HIT, deverá ser possível exportar as informações do registro coletado e do registro de referência.

4.2.9.9. O Aplicativo deve exibir uma confirmação do envio ou de falha do cadastramento ao Sistema Central do ABIS no momento do cadastramento e no histórico.

4.3. Previsão de inserções biométricas

4.3.1. A demanda de biometrias pendentes de comparação biométrica da Polícia Federal em junho de 2025 é composta por biometrias fornecidas mediante Acordos de Cooperação com as Unidades Federativas (20 milhões), dados biométricos de DENATRAM (36 milhões) e dados biométricos da CIN (29 milhões), totalizando 85 milhões.

4.3.2. A previsão para inclusão de registros biométricos represados e a inclusão dos dados rotineiros no sistema ABIS segue a tabela abaixo:

	Início do Contrato	**Ano 1**	**Ano 2**	**Ano 3**	**Ano 4**	**Ano 5**	**Ano 6**	**Ano 7**	**Ano 8**	**Ano 9**	**Ano 10**
Incremento de Pessoas	40,00	0,00	40,00	40,00	23,00	23,00	23,00	23,00	23,00	23,00	19,60
Incremento de Registros	46,00	0,00	46,00	46,00	26,45	26,45	26,45	26,45	26,45	26,45	22,54
Acumulado de Pessoas	40,00	40,00	80,00	120,00	143,00	166,00	189,00	212,00	235,00	258,00	277,60
Acumulado de Registros	46,00	46,00	92,00	138,00	164,45	190,90	217,35	243,80	270,25	296,70	319,24

5. Necessidades Tecnológicas

5.1. São necessários equipamentos como servidores e *storage* para garantir funcionamento da solução.

5.1.1. A especificação básica dos servidores homologados pela Diretoria de Tecnologia da Informação da Polícia Federal para o sistema ABIS é a seguinte:

Servidor de rede - *hipervisor* de VMs de correspondência do ABIS

a) Sistema operacional

i. O modelo do servidor ofertado deve ser certificado pela *Red Hat* como compatível com o sistema operacional *Red Hat Enterprise* Linux 9 ou posterior e deve ser certificado pela Microsoft como compatível com o sistema operacional Windows Server 2022 ou posterior.

b) Processadores

i. O servidor deve possuir 2 (dois) processadores com arquitetura Intel x86 de 64 bits e tecnologia de virtualização Intel VT-x ou AMD-V.

ii. O modelo de processador ofertado deverá possuir:

1. Núcleos: 32 (trinta e dois);

2. Memória cache L3: mínimo de 128 MB (cento e vinte e oito megabytes).

c) Memória

i. O servidor deve possuir no mínimo 2 TB (dois terabytes) de memória RAM, isto é, cada *socket* deverá ter no mínimo 1 TB (um terabyte).

ii. Os módulos de memória devem ser do padrão DDR5, LRDIMM ou RDIMM, com taxa de transferência de 4.800 (quatro mil e oitocentos) MT/s (milhões de transferências por segundo) ou superior, com detecção e correção de erros (ECC).

d) Gabinete

i. Deve ser próprio para montagem em *rack* padrão de 19 polegadas (*rackmount*), com altura máxima de 2U (duas rack units);

e) Fontes de alimentação

i. O servidor deve possuir 2 (duas) fontes de alimentação *hot-plug* redundantes.

f) Placa-mãe

i. Deve possuir controladora integrada de vídeo com, no mínimo, 16 MB (dezesseis megabytes) de memória, e deve suportar resolução de 1280x1024 em 60Hz;

ii. Deve possuir no mínimo 12 (doze) *slots* DIMM por *socket* para módulos de memória DDR5 ou superior.

g) Controladora RAID

i. O servidor deve possuir controladora RAID compatível com dispositivos de armazenamento dos tipos SATA de 6 Gbps ou superior e SAS de 12 Gbps ou superior;

ii. A controladora RAID deve:

1. Possuir memória cache de no mínimo 2 GB (dois gigabytes) com proteção por bateria ou memória não volátil;

2. Implementar RAID nos níveis 0, 1, 5, 6, 10, 50 e 60;

3. Permitir configurar unidades de armazenamento como *hot spare*;

h) Armazenamento

i. Unidades de *boot*

1. Quantidade: 2 (duas);

2. Tipo: SSD SATA de 6 Gbps ou superior;

3. Capacidade: 960 GB (novecentos e sessenta gigabytes) ou superior;

i) Controladoras de rede

i. O servidor deverá possuir as controladoras de rede a seguir:

1. Controladora de rede com no mínimo duas portas RJ-45 de 1 Gbps

    a. Quantidade: 1 (uma) controladora;

2. Controladora de rede com no mínimo duas portas SFP28 de 10/25 Gbps

    a. Quantidade: 1 (uma) controladora;

5.2. A quantidade de equipamentos é fortemente dependente do software da empresa contratada, uma vez que cada empresa apresenta tempos de resposta, consumo de memória RAM e armazenamento em base de dados diferentes, de acordo com relatórios NIST do teste ELFT.

5.3. O sistema central deverá possuir conjunto de APIs conforme Anexo VI. A contratada deverá disponibilizar as APIs e sua documentação.

5.4. Serão necessários os serviços de instalação, configuração, customização, migração, deduplicação, capacitação, manutenção e garantia.

5.5. Serviços Técnicos Especializados para a Implantação da Solução ABIS.

5.6. Serviços para Implantação da Solução ABIS com a atuação de equipes técnicas da contratante e da contratada.

5.7. Instalação e configuração de todos os softwares dos sistemas ABIS Central e clientes ABIS.

5.8. Adoção de um canal seguro, preferencialmente com criptografia de mercado, para a comunicação de dados entre os sistemas ABIS Central e clientes ABIS.

5.9. Provimento de recurso de backup e contingência para continuidade do negócio, dentro das políticas da DTI/PF.

5.10. Transferência de conhecimento para a PF, a fim de possibilitar a migração dos dados para uma base de padrão aberto possível de ser reconhecida por outros softwares e para minimizar eventual dependência tecnológica, além de viabilizar a migração dos dados para bases externas à solução para, por exemplo, inteligência analítica ou de negócio.

5.11. Entrega de uma solução em que a contratante possa executar, operar e sustentar sem a dependência exclusiva da empresa contratada ou do seu fabricante.

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

6.1. Requisitos de Negócios

6.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

6.1.2. Atualizar e adequar a capacidade de processamento, operação e armazenamento das identificações biométricas da Polícia Federal.

6.1.3. Garantir a não-interrupção dos serviços de identificação humana da Polícia Federal.

6.2. Requisitos de Capacitação

6.2.1. A CONTRATADA deverá observar o escopo das exigências técnicas demandadas e, deverá oferecer curso de capacitação em níveis operacional e técnico, contemplando visão geral da Solução.

6.2.2. Aspectos Administrativos

6.2.2.1. Durante a fase de elaboração do Projeto Executivo a CONTRATADA e a CONTRATANTE desenvolverão, em conjunto, o Plano de Capacitação e Treinamento da solução a ser implantada, que atenderá, no mínimo, as especificações dos Anexos I e II.

6.2.2.2. A CONTRATADA, previamente à realização de cada capacitação deverá elaborar e submeter para apreciação, análise e aprovação da CONTRATANTE o Plano de Ação Educacional, conforme Anexo III.

6.2.2.3. O início da prestação do serviço de capacitação se dará após a aprovação dos Planos de Ação Educacional por parte da CONTRATANTE.

6.2.2.4. Cada turma será solicitada pela CONTRATANTE por meio de ordem de serviço – OS –, a ser encaminhada à CONTRATADA por meio de ofício ou documento equivalente, com antecedência mínima de 15 (quinze) dias da data prevista de início da realização da capacitação.

6.2.3. Aspectos Operacionais

6.2.3.1. Os encontros de capacitação deverão ocorrer nas dependências da CONTRATANTE, presencialmente no horário comercial (08h00 às 18h00).

6.2.3.2. Os encontros de capacitação serão gravados pela CONTRATANTE. Todo material gravado será de propriedade da Polícia Federal e será de uso exclusivo dentro da própria instituição, de conhecimento integral dos servidores e prestadores de serviço envolvidos, sendo vedada qualquer possibilidade de transmissão, reprodução ou divulgação fora deste Órgão e a terceiros estranhos à execução do objeto contratual.

6.2.3.3. Toda e qualquer transmissão, reprodução ou divulgação a terceiros alheios ao contrato devem ter a autorização expressa da empresa contratada.

6.2.3.4. A CONTRATANTE disponibilizará estrutura com as seguintes características:

6.2.3.4.1. Sala compatível com a quantidade de treinandos;

6.2.3.4.2. Computadores com acesso ao ambiente de treinamento;

6.2.3.4.3. Projetor e *Data Show*;

6.2.3.4.4. Estrutura de gravação da capacitação;

6.2.3.5. As aulas de todas as turmas da capacitação deverão ser ministradas em Português do Brasil, por técnicos especializados na operação e administração da solução a ser implantada, de modo a facilitar o entendimento do conteúdo apresentado, utilizando-se de linguagem técnica e clara.

6.2.3.6. Caso o regente da aula não seja fluente em Português do Brasil, a CONTRATADA deverá providenciar tradutor fluente no idioma;

6.2.3.7. A qualquer tempo, o Fiscal do Contrato poderá solicitar comprovação de qualificação técnica de qualquer profissional que esteja atuando no contrato, podendo solicitar sua substituição em caso de desconformidade com as exigências feitas. A substituição dos profissionais indicados durante a execução do contrato somente será permitida por outros com qualificações iguais ou superiores às exigidas neste Termo de Referência e após aprovação pelo INI/DPA/PF ou pela DTI/PF.

6.2.4. Público-alvo e vagas

6.2.4.1. Deverão ser dois os níveis de capacitação: Operador de Sistema ABIS e Administrador de Sistema ABIS.

6.2.4.2. Deverão ser ofertadas duas turmas de 20 (vinte) alunos para a capacitação de Operadores do Sistema ABIS, com carga horária não inferior a 110 (cento e dez) horas em cada turma.

6.2.4.3. O público-alvo das turmas de capacitação de Operadores do Sistema ABIS serão Papiloscopistas Policiais Federais, instrutores do Instituto Nacional de Identificação da Polícia Federal, que posteriormente farão a remodelagem do curso, incluindo demais pontos de interesse da atividade e normativos e replicarão aos operadores dos Estados.

6.2.4.4. O CONTEÚDO MÍNIMO DO PLANO DE AULA do curso de capacitação de operador está descrito no ANEXO I, constituindo-se de uma lista de tópicos que deverão ser abordados nas aulas de maneira obrigatória, sendo direcionados de maneira técnica e precisa à solução a ser implementada.

6.2.4.5. Deverão ser ofertadas duas turmas de até 20 (vinte) alunos para a capacitação de Administradores do Sistema ABIS, com carga horária não inferior a 60 (sessenta) horas em cada turma.

6.2.4.6. O público-alvo das turmas de capacitação de Administrador do Sistema ABIS serão servidores e outros profissionais designados pela CONTRATANTE, a exemplo de prestadores de serviço da Polícia Federal, indicados pela da DTI/PF e pelo INI/DPA/PF, com experiência em TI, que posteriormente nortearão a administração do sistema.

6.2.4.7. O CONTEÚDO MÍNIMO DO PLANO DE AULA do curso de capacitação de administrador está descrito no ANEXO II, constituindo-se de uma lista de tópicos que deverão ser abordados nas aulas de maneira obrigatória, sendo direcionados de maneira técnica e precisa à solução a ser implementada.

6.2.4.8. Cada turma deverá possuir no máximo 20 (vinte) alunos inscritos.

6.2.5. Disponibilização do ambiente de treinamento e de materiais de apoio

6.2.5.1. As turmas da capacitação serão marcadas após a disponibilização do ambiente de treinamento e dos materiais de apoio.

6.2.5.2. Os materiais de apoio deverão abordar as características e funcionamento das tecnologias e serviços relacionados às soluções providas pela CONTRATADA, incluindo equipamentos, softwares e outros recursos utilizados, e seu teor deverá ser submetido à apreciação da CONTRATANTE para sua aprovação, devendo a CONTRATADA realizar as alterações solicitadas.

6.2.5.3. A CONTRATADA será responsável pelo fornecimento de todo material e documentação necessários à perfeita compreensão da solução instalada. Todos os materiais deverão ser fornecidos em Português do Brasil.

6.2.5.4. Todo material entregue será de propriedade da Polícia Federal e será de uso exclusivo dentro da própria instituição, de conhecimento integral dos servidores envolvidos e de todos os prestadores de serviço legalmente constituídos, sendo vedada qualquer possibilidade de transmissão, reprodução ou divulgação fora deste Órgão e a terceiros estranhos à execução do objeto contratual.

6.2.5.5. Toda e qualquer transmissão, reprodução ou divulgação a terceiros alheios ao contrato devem ter a autorização expressa da empresa contratada.

6.2.6. Conteúdo mínimo dos materiais de apoio

6.2.6.1. A CONTRATADA será responsável pelo fornecimento de todo material e documentação necessários à perfeita compreensão da solução instalada. Os materiais de apoio deverão ser disponibilizados de forma física e digital e serão constituídos por:

6.2.6.2. Manuais de usuário do sistema em português, divididos em níveis de usuário, que devem conter a descrição dos fluxos e os elementos e funcionalidades disponíveis na solução.

6.2.6.3. Manual de Operador: deverá conter toda a parte de usabilidade do operador e todas as informações sobre configurações do sistema, ilustrações com navegabilidade e procedimentos que podem ser realizados nas ferramentas. Deverão conter vídeos que demonstrem de maneira prática as principais ações e funcionalidades do sistema;

6.2.6.4. Manual de Administrador: mecanismos de manutenção dos serviços e auditoria da confiabilidade do algoritmo, bem como da integridade do banco. Também, deverá trazer diretrizes de segurança e privacidade, bem como a manutenção básica da solução e suporte;

6.2.6.5. Documentações técnicas em português de desenvolvimento com procedimentos padronizados para utilização de sistemas e equipamentos;

6.2.6.6. Documentação em português no momento de entrega do sistema ou do equipamento, sendo imprescindível para homologação e aceite por parte da CONTRATANTE;

6.2.6.7. Documentações em português dos aplicativos clientes, com os códigos-fontes dos aplicativos desenvolvidos para a CONTRATANTE e todos os fluxos e procedimentos, inclusive para instalação e desinstalação;

6.2.6.8. As apresentações em formato de slides, utilizadas nos cursos, na proporção de uma cópia por cada servidor participante da capacitação.

6.2.6.9. O curso de capacitação deverá ser apostilado, com a descrição detalhada em nível técnico e operacional, no idioma português do Brasil, abrangendo, no mínimo, os níveis de abordagem e tópicos descritos no CONTEÚDO MÍNIMO DO PLANO AULA (Anexos I e II).

6.2.7. Avaliação e aceite do curso

6.2.7.1. A CONTRATADA expedirá certificado de conclusão aos alunos que cumprirem os requisitos de aprovação e aproveitamento estabelecidos em cada turma (Anexo III).

6.2.7.2. A frequência do corpo discente e docente será comprovada, conforme o Anexo V.

6.2.7.3. Após a conclusão de cada turma de capacitação, apurados os resultados da avaliação, poderão ser solicitados ajustes na distribuição da carga-horária, estratégias pedagógicas, conteúdos e outros aspectos didático-pedagógicos para garantir o desenvolvimento das competências necessárias ao manejo da ferramenta.

6.2.7.4. A CONTRATADA deverá aplicar o formulário de avaliação da qualidade da ação educacional (Anexo IV) em cada capacitação, ao corpo discente, observando as especificações e orientações da CONTRATANTE.

6.2.7.5. A CONTRATADA deverá, sem ônus para a CONTRATANTE, realizar nova edição da capacitação quando na avaliação de qualidade da ação educacional da capacitação o critério “bom” for inferior a 70% (setenta por cento) das avaliações do corpo discente, no campo “Execução” (Anexo IV).

6.2.7.6. A CONTRATADA expedirá certificado de conclusão aos alunos que cumprirem os requisitos de aprovação e/ou aproveitamento estabelecidos em cada Plano de Ação Educacional (Anexo V).

6.2.7.7. A CONTRATADA deverá comunicar imediatamente a CONTRATANTE qualquer situação, fato ou evento que impeça ou interrompa a execução da capacitação, para que sejam realizados os ajustes necessários ao alcance dos objetivos educacionais.

6.2.7.8. Nesses casos, verificado que os objetivos pedagógicos não foram alcançados, a capacitação deverá ser refeita sem ônus para a CONTRATANTE.

6.2.7.9. O pagamento do item de capacitação está diretamente vinculado ao ACEITE da CONTRATANTE, que se dará por meio de relatório conclusivo ao final das capacitações, o qual avaliará se a capacitação foi realizada de maneira integral, levando em conta as avaliações realizadas ao final de cada turma da capacitação e os materiais de apoio ofertados pela CONTRATADA.

6.2.7.10. Em caso de capacitação incompleta ou insuficiente, deverá a CONTRATADA providenciar novas turmas com conteúdo adequado às exigências e necessidades técnicas e didáticas faltantes.

6.2.7.11. Todos os encargos e despesas para realização da capacitação serão de responsabilidade da CONTRATADA, inclusive aquelas decorrentes da eventual repetição da capacitação insatisfatória.

6.2.7.12. Em caso de interrupção, por motivos alheios à CONTRATANTE, e não se configurar hipótese para o refazimento da capacitação, não haverá qualquer pagamento.

6.2.7.13. Em caso de haver interrupção motivada pela CONTRATANTE, haverá suspensão da capacitação e retomada em momento oportuno, com o devido pagamento integral do item à CONTRATADA quando da finalização de todas as turmas previstas.

6.3. Requisitos Legais

6.3.1. Constituição Federal;

6.3.2. Lei nº 14.133/2021;

6.3.3. Instrução Normativa SGD/ME nº 94, de 2022;

6.3.4. Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021;

6.3.5. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

6.3.6. Decreto 10.024, de 20 de setembro de 2019;

6.3.7. Guia Nacional de Contratações Sustentáveis;

6.3.8. Guia de Requisitos e Obrigações Quanto a Privacidade e à Segurança da Informação;

6.3.9. Decreto n° 11.462, de 31 de março de 2023;

6.4. Requisitos de Garantia, Manutenção e Assistência Técnica

6.4.1. A Solução deve ser adquirida com garantia ao longo de toda a vigência do contrato.

6.4.2. É necessária a transferência de conhecimento para a instalação e configuração dos sistemas clientes.

6.4.3. Devido às características da solução, há necessidade de realização de manutenção pela CONTRATADA, visando garantir disponibilidade da solução.

6.4.4. A Solução ABIS atual, referente ao Contrato 01/2021-DTI/PF, não houve item de manutenção e acarretou indisponibilidade do sistema por semanas em 2025.

6.4.5. Estes requisitos definem a forma como será conduzida o acionamento da garantia e a comunicação entre as partes envolvidas devem seguir os seguintes requisitos:

6.4.5.1. O prazo da garantia está definido nos requisitos temporais deste Estudo e as coberturas referentes à Garantia dossoftwarecontratados estender-se-ão por tempo que será definido posteriormente, contado da data do Aceite da solução.

6.4.5.2. A prestação da garantia deverá contemplar o cumprimento de Níveis Mínimos de Serviço que considerem pelo menos agradação de severidade, os tempos de solução definitiva, solução de contorno e prazos de atendimento.

6.4.5.3. A Garantia deverá cobrir todos os itens desoftware, assegurando que a Solução continuará atendendo a todos os requisitos descritos no presente Documento durante o período de cobertura sem custos adicionais para a CONTRATANTE, desde que não seja constatado mau uso de algum componente da Solução.

6.4.5.4. De maneira similar, caso sejam identificadas desconformidades nas adaptações, implementações e configurações dossoftwares, durante o período de Garantia, a CONTRATADA deverá se responsabilizar pelas corre ções.

6.4.5.5. Para abertura, acompanhamento e atendimento de chamados emgarantia, a CONTRATADA deverá disponibilizar Central de Atendimento Telefônico e Sistema de Abertura de Chamados viaweb, que deverão estar disponíveis 24 horas por dia, 7 dias por semana, com atendimentos em português do Brasil.

6.4.5.6. A Central de Atendimento deverá ser acessada por um número único nacional exclusivo para a CONTRATANTE ou corporativo com chave de acesso exclusiva.

6.4.5.7. A CONTRATADA deverá atender aos chamados de acordo com os Níveis Mínimos de Serviço previamente estabelecidos. Caso os prazos de atendimento não sejam cumpridos, a contratada deverá sofrer redimensionamento na fatura referente à ocorrência do descumprimento e o percentual será aplicado sobre o valor da respectiva fatura. Em caso de descumprimento após a vigência contratual e da garantia de execução, será instaurado processo administrativo resguardando a ampla defesa e o contraditório conforme legislação vigente.

6.4.5.8. A CONTRATANTE terá o direito de receber, durante a vigência da Garantia, todas as atualizações de softwareenvolvendo os produtos licenciados na presente contratação. Deverão ser disponibilizadas todas as atualizações dentro da mesma versão de referência(update), cabendo à Administração avaliar a oportunidade e a conveniência da implantação da atualização disponibilizada.

6.4.5.9. O atendimento para os elementos desoftwareda Soluçãopoderá ser remoto ou presencial, dependendo da gravidade do chamado. Os atendimentos presenciais ocorrerão exclusivamente em Brasília – DF.

6.4.5.10. A CONTRATADA deverá informar proativamente à CONTRATANTE sobre a descoberta de erros(bugs), vulnerabilidades e as suas respectivas correções nossoftwarerelacionados nesta contratação, durante toda a vigência contratual.

6.4.5.11. A garantia deverá cobrir ainda, relacionados aatividades de implantação:

6.4.5.11.1. resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades relacionadas a cadasoftwarecomponente da Solução;

6.4.5.11.2. resolução de problemas de desempenho e estabilidade do ambiente;

6.4.5.11.3. resolução de problemas que limitem ou impeçam o desenvolvimento ou a execução das aplicações da CONTRATADA que façam uso efetivo das funcionalidades desoftwareque compõem a Solução.

6.4.5.12. A CONTRATADA somente poderá finalizar cada atendimento efetuado após a homologação formal do responsável técnico da CONTRATANTE, ou se após a conclusão do chamado a CONTRATANTE ficar mais de 15 (quinze) dias sem atualizar o chamado que originou o atendimento sem aviso prévio.

6.4.5.13. A conclusão do chamado deverá contemplar emissãode relatório técnico conclusivo da causa do problema e da solução que foi adotada para o seu restabelecimento, apresentando no mínimo:

6.4.5.13.1. número do chamado;

6.4.5.13.2. data e hora do chamado;

6.4.5.13.3. data e hora do início e término do atendimento;

6.4.5.13.4. total de horas utilizadaspara atendimento completo;

6.4.5.13.5. severidade do erro;

6.4.5.13.6. identificação do problema;

6.4.5.13.7. solução de contorno, se aplicável;

6.4.5.13.8. solução definitiva, se aplicável.

6.4.6. A manutenção deve seguir os requisitos que serão definidos posteriormente.

6.5. Requisitos Temporais

6.5.1. Sistemas ABIS apresentam tempos de implantação longos, a exemplo do sistema ABIS atual demandou 15 meses para a operacionalização (GO Live) e 12 meses para o aceite definitivo, totalizando 27 meses desde a assinatura do contrato. Tendo em vista o tempo de implantação, espera-se que o sistema contratado seja utilizado pelo período de 10 anos se atendidos os requisitos legais para as respectivas prorrogações contratuais.

6.5.2. Os requisitos temporais a respeito de Projeto Executivo, instalação, configuração, customização, migração e deduplicação serão definidos após diálogo com as empresas do setor.

6.6. Requisitos de Segurança e Privacidade

6.6.1. A contratada deverá entregar junto com a formalização contratual o Termo de Manutenção de Sigilo, conforme modelo disponibilizado pela contratante.

6.6.2. A contratada deverá manter em caráter confidencial, através de Termo de Manutenção de Sigilo, mesmo após o término do prazo de vigência ou eventual rescisão do contrato, todas as informações a que teve acesso.

6.6.3. A contratada deverá fornecer documentação para credenciamento das equipes de atuação na contratante.

6.6.4. A solução deverá aderir aos princípios e procedimentos elencados no plano de segurança da Informação da PF, como disponibilidade, controle de acesso e verificações de integridade, além de:

6.6.4.1. Adoção de boas práticas de manutenção periódica, com gestão de patches, backup regular e monitoramento contínuo.

6.6.4.2. Registro de falhas, com logs de auditoria, monitoramento de eventos e análise de incidentes.

6.6.4.3. Controles no envio de informações, com criptografia de dados, autenticação, e controle de acesso e permissões.

6.6.5. Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.

6.6.6. A Contratada se comprometerá a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.

6.6.7. A solução deverá prever a geração de trilhas de auditoria para todas as operações de inclusão, exclusão, alteração de dados, desligamento do ambiente e alteração de configuração da plataforma. As informações de auditoria deverão estar disponíveis por meio de relatórios específicos.

6.6.8. A Solução deverá conter funcionalidade de login por confirmação biométrica facial ou senha de acesso única a cada operador.

6.6.9. Após transcurso de dado lapso temporal de total inatividade, a aplicação deverá encerrar a sessão inerte, retornado à condição de login necessário e confirmado por biometria facial ou senha de acesso.

6.6.10. A Contratada deve possuir Política de Segurança Cibernética (PSC) ou equivalente, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas, com processo de revisão periódica formalizado e institucionalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança cibernética para assegurar a consistência, a privacidade e a confiabilidade dos dados e informações que trafegam no objeto contratado.

6.6.11. A Contratada deverá realizar, em conjunto com a Contratante, análise de impacto na privacidade dos dados pessoais relacionada ao objeto da contratação, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço.

6.6.12. A Contratada deverá realizar e apresentar à Contratante periodicamente uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados ao objeto do contrato, indicando o nível de risco ao qual o objeto do contrato e a Contratante está exposta, baseada em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela Contratante.

6.6.13. A Contratada deverá apresentar, em tempo determinado pela Contratante:

6.6.13.1. Documentação que descreve a arquitetura física e lógica do objeto;

6.6.13.2. Uma descrição dos controles de segurança cibernética implementados em cada componente descrito na arquitetura física e lógica;

6.6.13.3. Matriz de responsabilidades descrevendo os papéis e suas respectivas responsabilidades pela segurança cibernética relacionada ao objeto da contratação e com relação aos itens aqui descritos.

6.6.14. A Contratada deverá utilizar recursos de segurança cibernética e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e, sempre que possível, em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a Contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela Contratante.

6.6.15. A Contratada deverá assegurar que os ambientes tecnológicos de desenvolvimento, teste, homologação e produção estejam segregados e possuam controles de segurança cibernética adequados a cada ambiente, de forma a para reduzir o nível de riscos de acessos ou modificações não autorizadas.

6.6.16. A Contratada deverá possuir e implementar processo de gestão de mudanças adequado para que mudanças na organização, nos processos de negócio e nos recursos de processamento da informação sejam controlados e não afetem a segurança cibernética, reduzindo o nível de risco ao qual o objeto do contrato e/ou a Contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela Contratante.

6.6.17. A Contratada deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e as medidas tomadas para mitigá-los e evitar reincidências; além de implementar e manter controles e procedimentos específicos para detecção, tratamento e resposta a incidentes de segurança cibernética, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a Contratante está exposto, considerando os critérios de aceitabilidade de riscos definidos pela Contratante.

6.6.18. A Contratada deve implementar os controles necessários para o registro de eventos e incidentes de segurança cibernética.

6.6.19. A Contratada deve reportar de imediato à Contratante incidentes que envolvam vazamento de dados, fraude ou comprometimento da informação relacionados ao objeto do contrato.

6.6.20. A Contratada deve implementar os controles necessários para coleta e preservação de evidências de incidentes de segurança.

6.6.21. A Contratada deverá implementar controles de acesso baseado em uma política de controle de acesso para o objeto contratado, elaborada pela Contratante em conjunto com a Contratada, tendo em vista o princípio do menor privilégio e a proteção adequada aos dados pessoais, de forma a reduzir o nível de risco ao qual o objeto e a Contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela Contratante. A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política. A política também deve definir situações e protocolos para acesso a informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos e que a Contratante julgar necessário.

6.6.22. A Contratada deverá apresentar à Contratante, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

6.6.23. A Contratada deverá disponibilizar todos os recursos necessários para que a Contratante, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança cibernética relacionadas ao objeto do contrato.

6.6.24. A Contratada deve implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança cibernética, aderente a disposto em dispositivo legal correlato publicado pelo GSI /PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à Contratante para fins de auditorias e inspeções.

6.6.25. A Contratada deve implementar medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (*logs*) de suas próprias atividades.

6.6.26. A Contratada deve implementar e manter controles e procedimentos específicos para assegurar o completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da Contratada venham tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da solução objeto do contrato, cumprindo e fazendo cumprir o disposto nos acordos de confidencialidade firmados.

6.6.27. A Contratante deverá comunicar à Contratada, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da Contratante, porventura colocados à disposição para realização dos serviços contratados.

6.7. Requisitos Sociais e Culturais

6.7.1. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

6.7.2. Utilização de uniformes e crachá, nas dependências da contratada.

6.7.3. Todas as interfaces do software e seus materiais de apoio (manuais, tutoriais, comunicações automatizadas) devem ser elaborados em Língua Portuguesa;

6.7.4. É preferível soluções desenvolvidas por empresas que adotem práticas de Responsabilidade Social Corporativa e mantenham políticas de diversidade, equidade e inclusão;

6.7.5. A empresa deverá implantar Programa de Integridade ou adequar seu Programa de Integridade conforme Portaria 513/2020 do Ministério da Justiça e Segurança Pública.

6.8. Requisitos da Arquitetura Tecnológica

6.8.1. A utilização de um SGBD relacional para o sistema ABIS e as licenças de SGBD Oracle Database Enterprise Server ou Microsoft SQL Enterprise Server para o número de processadores necessários devem ser fornecidas pela CONTRATADA.

6.8.1.1. As licenças de SGBD não devem ser do tipo banco de dados incorporado (Embedded Database) ou similar, a fim haver menor dependência entre o banco de dados e a aplicação e de viabilizar a manutenção das bases e a extração dos dados para bases externas diretamente pela contratante.

6.8.1.2. Não deve haver restrição à extração ou exportação direta dos dados para outros gerenciadores de banco, pelo menos para PostgreSQL e Microsoft SQL Server, devendo a eventual conversão dos dados no caso ser feita pela Contratante;

6.8.1.3. Nem mesmo o acesso por meio de software desenvolvido pela CONTRATADA será admitido para suprir a necessidade dos subitens anteriores.

6.8.2. Devem ser disponibilizados mecanismos para a CONTRATANTE monitorar plenamente a infraestrutura de aplicação, especialmente quanto ao uso de recursos (processamento, memória, armazenamento, por exemplo), por meio das seguintes possibilidades de monitoramento dos seus componentes de software:

6.8.2.1. Monitoramento através da geração de logs de eventos;

6.8.2.2. Monitoramento através do protocolo SNMP;

6.8.2.3. Monitoramento através de agentes de software.

6.8.3. Deve ser possível integrar os mecanismos de monitoramento mencionados acima com outras plataformas de monitoramento e de gerenciamento de eventos já adotadas pela CONTRATANTE.

6.9. Requisitos de Projeto e de Implementação

6.9.1. A solução deverá observar integralmente os requisitos de projeto e de implementação descritos a seguir:

6.9.2. Assinatura do contrato;

6.9.3. Realização de Projeto Executivo;

6.9.4. Instalação e Configuração dos Ambientes de Produção, Homologação, Treinamento e Testes;

6.9.5. Migração e Deduplicação de dados biométricos;

6.9.6. Instalação e Configuração de Softwares Clientes;

6.9.7. Capacitação (após entrega do Ambiente de Treinamento);

6.10. Requisitos de Implantação

6.10.1. A solução deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

6.10.2. A instalação e configuração do Sistema ABIS Central deverá ser instalado na sala cofre da Diretoria de Tecnologia da Informação e Inovação – DTI/PF – em Brasília, Distrito Federal, localizada no SAIS Quadra 7 - Lote 23 - Setor Policial Sul Brasília-DF / CEP 70610-902.

6.10.3. A instalação e configuração de Sistemas Clientes será realizada de forma remota em computadores da Polícia Federal fora do Distrito Federal.

6.10.4. Deverá ser realizada transferência de conhecimento da instalação e configuração de Sistemas Clientes com demonstração prática e manuais atualizados.

6.11. Requisitos de Experiência Profissional

6.11.1. A empresa deverá demonstrar já ter fornecido sistema de identificação biométrica capaz de realizar pesquisas de impressão digital, impressão palmar, face e impressões latentes. O atestado deverá ser emitido por instituição de direito público ou privado, nacional ou estrangeira.

6.12. Requisitos de Formação da Equipe

6.12.1. Não serão exigidos requisitos de formação da equipe para a presente a contratação, sendo exigido o atendimento das capacidades, transações diárias e tempos de resposta.

6.12.2. O preço de serviço, no que se refere a equipe, deverá observar a formação de preço em função do cargo do integrante da equipe conforme a Portaria SGD/MGI Nº 6.680, DE 4 DE OUTUBRO DE 2024.

6.13. Requisitos de Metodologia de Trabalho

6.13.1. A metodologia de trabalho para as etapas de instalação, configuração, customização, migração e deduplicação serão definidos após diálogo com as empresas do setor.

6.13.2. A metodologia de trabalho para o serviço de capacitação será realizada de acordo com os item 6.2.

6.13.3. A metodologia de trabalho referente a manutenção e garantia será através da abertura chamados através de Sistema de Abertura de Chamados via web e de Central de Atendimento Telefônico fornecidos pela contratada, que deverão estar disponíveis 24 horas por dia, 7 dias por semana, com atendimentos em português do Brasil.

6.14. Requisitos de Segurança da Informação e Privacidade

6.14.1. A solução deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

6.14.2. A contratação deverá estar alinhada com a Lei Geral de proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018;

6.14.3. A contratada deverá apresentar documento de Política de Segurança da Informação (POSIN), na assinatura do Contrato. A POSIN tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, sistemas, documentos, correspondências e publicações, que estejam envolvidos na contratação;

6.14.4. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Cibernética da Polícia Federal.

6.15. Outros Requisitos Aplicáveis

6.15.1. A ser definido.

6.16. Requisitos de Sustentabilidade

6.16.1. 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:

6.16.2. A empresa contratada deverá contribuir para o descarte de equipamentos e bens de informática da administração pública direta de maneira correta e sustentável como prevê a Lei n° 14.479 de 2022;

6.16.3. Somente poderão ser utilizados na execução dos serviços bens de informática e/ou automação que possuam a certificação de que trata a Portaria INMETRO nº 304, de 2023 ou que possuam comprovada segurança, compatibilidade eletromagnética e eficiência energética equivalente;

6.17. Indicação de marcas ou modelos **(Art. 41, inciso I, da Lei nº 14.133, de 2021)**

6.17.1. Não se aplica a essa contratação.

6.18. Da vedação de utilização de marca/produto na execução do serviço

6.18.1. Não se aplica a essa contratação.

6.19. Da exigência de carta de solidariedade

6.19.1. Não se aplica a essa contratação.

6.20. Subcontratação

6.20.1. Não se aplica a esta contratação, no aspecto de infraestrutura de TIC.

6.20.2. Poderá ser aprofundado após discussão das soluções e após o diálogo com as empresas.

6.21. Da verificação de amostra do objeto

6.21.1. Não será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados.

6.22. Requisitos de garantia da contratação

6.22.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

6.22.2. Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

6.22.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

6.22.4 O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Itens previstos para atendimento da Demanda:

Item	Descrição	Quantidade
Item 1	Solução de Sistema Automatizado de Identificação Biométrica (ABIS) com capacidade para 277 milhões de pessoas	01 unidade
Item 2	Licenças flutuantes para Estação de Trabalho Pericial	537 unidades
Item 3	Licenças flutuantes para Estação de Cadastramento	XX unidades
Item 4	Licenças flutuantes para Dispositivos Móveis	XX unidades

Item 5	Serviço de Migração de dados	01 unidade
Item 6	Serviço de Deduplicação de dados	01 unidade
Item 7	Serviço de Capacitação dos servidores da CONTRATANTE	01 unidade
Item 8	Serviço de Manutenção do Sistema	XX meses

7.2. Memória de cálculo

7.2.1. Capacidade de Pessoas no Sistema ABIS:

7.2.1.1. Cálculo da População Brasileira (incluindo menores de 12 anos) até 2035[1]: 219.367.247;

7.2.1.2. Acumulado de brasileiros mortos entre 1996 e 2035[2]: De 1996 a 2023, 32.743.259, de 2024 até 2035, 20.219.484 (estimativa por regressão linear). Total de 52.962.743;

7.2.1.3. Estrangeiros presentes no ABIS[3] e com entrada até 2035[4]: atualmente o ABIS contém 2.533.075 estrangeiros individualizados (de um conjunto de 3.379.426 registros de estrangeiros) e estima-se que o número de estrangeiros no SISMIGRA entre 2025 e 2035 seja de 2.727.021 (estimativa por regressão linear). Total de 5.260.096.

7.2.1.4. Portanto, a capacidade necessária de pessoas individualizadas é de **277.590.086**. Mantida a proporção de Registros de Passagem e de Registros de Pessoa de 1,15, o total de registros de Passagem será de 319,2 milhões.

7.2.2. Número de Licenças flutuantes para Estação de Trabalho Pericial

7.2.2.1. Número está vinculado ao quantitativo de postos ocupados de Papiloscopistas Policiais Federais.

7.2.3. Número de Licenças flutuantes para Estação de Cadastramento e para Dispositivos Móveis

7.2.3.1. O quantitativo de licenças baseia-se no quantitativo da solução anterior e no levantamento atual da demanda conforme a tabela abaixo:

Unidades da Polícia Federal	Demanda do Contrato 01/2021 DTI/PF		Levantamento da demanda atual	
	Estação de Cadastramento	Dispositivos Móveis	Estação de Cadastramento	Dispositivos Móveis
SR/PF/AC	5	5	XX	XX
SR/PF/AL	9	6	XX	XX
SR/PF/AM	11	3	XX	XX
SR/PF/AP	5	5	XX	XX
SR/PF/BA	10	9	XX	XX
SR/PF/CE	5	4	XX	XX
SR/PF/DF	6	3	XX	XX

SR/PF/ES	5	5	XX	XX
SR/PF/GO	5	5	XX	XX
SR/PF/MA	4	5	XX	XX
SR/PF/MG	43	25	XX	XX
SR/PF/MS	10	16	XX	XX
SR/PF/MT	9	7	XX	XX
SR/PF/PA	9	8	XX	XX
SR/PF/PB	6	3	XX	XX
SR/PF/PE	7	5	XX	XX
SR/PF/PI	12	5	XX	XX
SR/PF/PR	15	13	XX	XX
SR/PF/RJ	20	7	XX	XX
SR/PF/RN	6	4	XX	XX
SR/PF/RO	9	3	XX	XX
SR/PF/RR	16	5	XX	XX
SR/PF/RS	18	16	XX	XX
SR/PF/SC	15	9	XX	XX
SR/PF/SE	3	4	XX	XX
SR/PF/SP	50	39	XX	XX
SR/PF/TO	7	3	XX	XX
INI/DPA/PF e outros Órgãos Centrais	20	45	XX	XX
TOTAL	340	267	XX	XX

8. Levantamento de soluções

8.1. Solução 1: Software Público

8.1.1. Regido pela Portaria STI/MP n° 46, de 28/09/2016 (alterada pela Portaria SGD/ME n° 3, de 27/06/2019), o Portal de Software Público Brasileiro oferece soluções em software livre que atendem às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.

8.1.2. Em pesquisa no Catálogo de Software Público, não foi encontrada solução que atendesse as necessidades desta contratação.

8.2. Solução 2: Software Livre

8.2.1. Os softwares livres para comparação biométrica encontrados foram o NBIS (NIST Biometric Image Software), que utiliza NFSEG e BOZORTH3, e o SourceAFIS. Esses softwares não se encaixam nas exigências de capacidade, requisitos funcionais e acurácia, além da necessidade de suporte ou desenvolvimento complementar.

8.2.2. Dessa forma, nao existe software livre que atenda a todos os requisitos da Polícia Federal.

8.3. Solução 3: Ampliação da Solução Implantada

8.3.1. Possibilidade de ampliação da solução implantada e adaptação aos novos requisitos será esclarecida diálogo com a empresa do sistema atual.

8.4. Solução 4: Aquisição de Software

8.4.1. A aquisição de software foi a solução aplicada na contratação 01/2021 - DTI/PF, sendo o hardware adquirido separadamente.

8.4.2. A compra de hardware anterior a compra de software ABIS é inviável em função da dependência entre o software e o quantitativo de hardware. A compra de hardware separada apresenta risco de ser inferior ao quantitativo de hardware necessário, como também apresenta risco de ser superestimada. O processo de compra de hardware e a viabilidade orçamentária posterior a contratação do software ABIS podem implicar em atraso na implantação do Sistema.

8.4.3. O incremento de hardware pela Polícia Federal precisa de Serviço Técnico Especializado da empresa fornecedora do ABIS para adaptação do sistema aos novos hardwares e pode apresentar risco de incompatibilidade entre hardwares antigos e novos.

8.5. Solução 5: Serviço Integrado

8.5.1. O serviço de solução integrada é composto por hardware, software e serviços. A empresa que irá projetar solução, fornecer hardware, software e serviço dentro das dependências da Polícia Federal e a infraestrutura de hardware e software permanece de posse da contratada, que disponibiliza e cobra pelo acesso aos serviços.

8.6. Solução 6: Aquisição Integrada

8.6.1. A aquisição de solução integrada é composta por hardware, software e serviços. A empresa que irá projetar solução, fornecer hardware, software e serviço dentro das dependências da Polícia Federal. Nessa solução, a infraestrutura de hardware e software pertencem a Polícia Federal após a implantação.

8.7. Solução 7: Contratação com Empresa Pública

8.7.1. Não é conhecida empresa pública que desenvolva sistemas ABIS com capacidade e acurácia para atender a demanda da Polícia Federal, portanto a contratação por empresa pública seria através de uma subcontratação, a exemplo

dos contratos da Perícia Forense do Estado do Ceará (PEFOCE) e da Polícia Civil do Distrito Federal (PCDF) com a Empresa de Tecnologia da Informação do Ceará (ETICE). Essas contratações foram realizadas na modalidade de serviço, semelhante a Solução 5.

8.7.2. Contratação com empresa pública será mais explorada na fase de diálogo com as empresas.

9. Análise comparativa de soluções

A ser definido.

10. Registro de soluções consideradas inviáveis

A ser definido.

11. Análise comparativa de custos (TCO)

A ser definido.

12. Descrição da solução de TIC a ser contratada

A ser definido.

13. Estimativa de custo total da contratação

Valor (R$): 1,00

A ser definido.

14. Justificativa técnica da escolha da solução

A ser definido.

15. Justificativa econômica da escolha da solução

A ser definido.

16. Benefícios a serem alcançados com a contratação

A ser definido.

17. Providências a serem Adotadas

A ser definido.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A ser definido pela EPC.

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.

CLAUBER FRANCO MIRANDA

Integrante Requisitante Substituto da EPC

Assinou eletronicamente em 06/08/2025 às 16:23:44.

SAULO GIOVANI DE MATOS SILVA

Integrante Técnico Titular da EPC

Assinou eletronicamente em 06/08/2025 às 16:21:02.

JOAO CESAR DE OLIVEIRA

Integrante Técnico Títular da EPC

ADEMIR DIAS CARDOSO JUNIOR

Autoridade competente

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - PERGUNTAS_PARA_A_CONSULTA_PUBLICA.pdf (83.95 KB)
- Anexo II - Anexos_ETPAnexos.pdf (157.34 KB)