**ESTUDO TÉCNICO PRELIMINAR**

**MINUTA**

| Versão do documento | Data da versão | Modificações |
|---|---|---|
| Versão 1 | 06/08/2025 | Documento disponibilizado para Consulta Pública. |
| Versão 2 | 07/11/2025 | Documento disponibilizado para Audiência Pública. |
| Versão 3 | 19/12/2025 | Documento disponibilizado após Audiência Pública. |

1. **INFORMAÇÕES BÁSICAS**
   1.1. 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<br><br>Objetivo Estratégico 4: Formar a polícia do futuro, moderna e inovadora<br><br>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<br><br>Objetivo Estratégico 3: Fortalecer a prevenção e o enfrentamento à criminalidade.<br><br>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 nº 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 se 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**

3.1. INI/DPA/PF

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 | - | 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 e FF/FF realizadas no momento da inserção de registro no ABIS. Não será realizada a pesquisa PER/PER do tipo PP/PP na inserção do registro, porém as impressões palmares que constarem dos prontuários inseridos poderão ser pesquisadas contra as latentes de palma e deverão também ser pesquisáveis por casos periciais.

4.1.1.3. Pesquisa sem Inserção (*Search-only*): O sistema deverá possibilitar a realização de pesquisas biométricas na modalidade *search-only*, nas quais os dados biométricos submetidos à consulta sejam utilizados exclusivamente para fins de comparação, sem a criação ou a persistência de registro biométrico no banco de dados do comparador após a conclusão da pesquisa. Os dados biométricos pesquisados não deverão ser disponibilizados ao usuário ao término da operação, sendo mantido apenas o registro de log para fins de auditoria, conforme as políticas de segurança e rastreabilidade do sistema ABIS. Essa funcionalidade deverá estar disponível para pesquisas utilizando impressões digitais, impressões palmares e reconhecimento facial, de forma conjunta ou 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 (1 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 SMT (*scars, marks, tattoos*); 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 LP/PP: 50 por dia;
4.1.3.7. Pesquisas PP/ULP: 50 por dia;
4.1.3.8. Pesquisas ULP/ULP: 50 por dia;
4.1.3.9. Pesquisas UFACE/FACE: 3000 por dia;
4.1.3.10. Pesquisas FACE/UFACE: 3000 por dia;
4.1.3.11. 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: 30 minutos;
4.1.4.5. Pesquisas LT/UL: 3 minutos;
4.1.4.6. Pesquisas LP/PP: 30 minutos;
4.1.4.7. Pesquisas PP/ULP: 30 minutos;
4.1.4.8. Pesquisas ULP/ULP: 30 minutos;
4.1.4.9. Pesquisas UFACE/FACE: 3 minutos;
4.1.4.10. Pesquisas FACE/UFACE: 3 minutos;
4.1.4.11. 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” (285 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 (investigation), 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), ou seja, quando a biometria de entrada divergir da biometria armazenada vinculada ao mesmo identificador. A Solução encaminhará o registro para análise manual e o usurário avaliará a origem da inconsistência e a necessidade de retificação ou desvinculação do identificador externo em 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 deverão 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. Processamento automatizado de minúcias: deve ser possível plotar automaticamente as minúcias sobre a imagem processada, utilizando o padrão de cores GYRO para facilitar a identificação visual e a análise detalhada dos pontos característicos.

4.1.6.7. Documentação detalhada do processo de análise: o sistema deve dispor de campos específicos para registrar informações complementares, como tipo de padrão, substrato, técnica de processamento e método de preservação. Esses dados precisam ser organizados para permitir o processamento futuro, consultas e geração de relatórios de maneira eficiente e estruturada.

4.1.6.8. *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.

4.1.6.9. *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.

4.1.6.10. 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;

4.1.6.11. Os dados biométricos de indivíduos com idade inferior a 7 anos completos deverão ser armazenados, processados e comparados exclusivamente dentro de um bloco lógico dedicado a essa faixa etária. Da mesma forma, os dados biométricos de indivíduos com idade igual ou superior a 7 anos deverão ser tratados em bloco próprio, com comparações restritas ao universo correspondente. Não deverá haver intercâmbio direto de dados biométricos entre os blocos etários. As comparações biométricas deverão ocorrer exclusivamente dentro do respectivo bloco, de modo a evitar correlações indevidas. A separação lógica entre os blocos visa mitigar os riscos decorrentes da instabilidade morfológica característica da infância, prevenindo falsos positivos, duplicidades e inconsistências que possam comprometer a acurácia do sistema. Pessoas inseridas sem o dado identificativo referente a idade deverão integrar o bloco de pessoas com idade superior a 7 anos.

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. Licenças dos Softwares clientes devem estar sem restrições artificiais que dificultem seu uso, re-instalação ou migração. Portanto, não devem utilizar:

4.2.2.1. Dispositivos físicos de proteção como dongles, hardlocks, tokens USB, etc.;

4.2.2.2. Vinculação ao hardware via serial number, MAC address ou ID de equipamento.

4.2.3. Todo o licenciamento necessário para funcionamento completo dos Sistemas Clientes deve estar incluído na proposta, incluindo eventuais componentes de terceiros.

4.2.4. 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.

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

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

4.2.7. 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.

4.2.8. Software para Estação de Trabalho Pericial

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

4.2.8.2. 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.

4.2.9. Software para Estação de Cadastramento

4.2.9.1. 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:

4.2.9.2. 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;

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

4.2.9.4. funcionar de maneira assíncrona, ou seja, a funcionalidade deverá ter a capacidade de trabalhar *offline* 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;

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

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

4.2.9.7. 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;

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

4.2.10.1. 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.

4.2.10.2. 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.

4.2.10.3. 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.

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

4.2.10.4.1. 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.

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

4.2.10.4.3. 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.

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

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

4.2.10.5.1. 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;

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

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

4.2.10.5.4. 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.

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

4.2.10.7. 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.

4.2.10.8. 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.

4.2.10.9. 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. Unidades de Serviço Técnico (UST)

4.3.1. Deverá ser prevista a disponibilização de Unidades de Serviço Técnico (UST), mensuradas em horas técnicas, destinadas ao atendimento de demandas de desenvolvimento, customização posterior, integração com sistemas parceiros ou outras alterações de escopo que venham a surgir ao longo da vigência contratual, após o início do Serviço de Comparação Biométrica, com a finalidade de assegurar a adequada adaptação da solução ABIS às necessidades institucionais da Polícia Federal. Tais serviços não se confundem com as atividades inerentes à implantação, configuração, customização inicial ou manutenção da solução, as quais permanecem integralmente contempladas no escopo principal da contratação.

4.3.2. Estima-se a necessidade de até 35.700 (trinta e cinco mil e setecentas) horas técnicas, a serem executadas por profissionais especializados na solução fornecida, acionadas sob demanda da Polícia Federal mediante emissão de Ordens de Serviço específicas, com definição prévia de escopo, entregáveis, prazos e quantitativos de horas. O pagamento será realizado exclusivamente com base nas horas efetivamente executadas e devidamente aceitas pela Administração, após validação das entregas correspondentes.

4.4. Previsão de inserções biométricas

4.4.1. 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.

4.4.2. 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. **NECESSIDADE TECNOLÓGICA**

5.1. Os equipamentos como servidores e *storage* deverão ser fornecidos pela empresa contratada, para garantir o funcionamento da solução.

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. O sistema ABIS Central e os sistemas clientes deverão ser disponibilizados em arquitetura web, acessíveis por navegador compatível, sem necessidade de instalação de software local nas estações de trabalho.

5.8. Os sistemas Clientes para estação de cadastramento e estação pericial deverão ser webservice.

5.9. A contratada será responsável pelo pleno funcionamento de todos os componentes do sistema tanto no ambiente central quanto nas estações clientes, garantindo o desempenho e a estabilidade da solução durante as etapas de instalação, configuração, customização e migração.

5.10. A solução deverá ser implantada integralmente pela contratada, incluindo integração com dispositivos biométricos existentes e compatibilidade com navegadores e sistemas operacionais utilizados pela Polícia Federal.

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

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

5.13. 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.

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:

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

6.1.1.2. 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 nº 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. 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.

6.4.4. Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativas/evolutivas) pela Contratada, visando a manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades de modo contínuo, como preceituado no art. 16, inciso I, alínea d da IN SGD/ME nº 94 de 2022.

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 dos softwares contratados estender-se-ão por tempo que será definido posteriormente, contados 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 de software, 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 dos softwares, durante o período de Garantia, a CONTRATADA deverá se responsabilizar pelas correções.

6.4.5.5. Para abertura, acompanhamento e atendimento de chamados em garantia, a CONTRATADA deverá disponibilizar Central de Atendimento Telefônico e Sistema de Abertura de Chamados via web, 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 contratual, todas as atualizações de software envolvendo 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 de software da Solução poderá 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 nos softwares relacionados nesta contratação, durante toda a vigência contratual.

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

6.4.5.11.1. resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades relacionadas a cada *software* componente 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 de software que 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 emissão de 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 do término do atendimento;

6.4.5.13.4. total de horas utilizadas para 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 do sistema visa garantir a continuidade e o adequado funcionamento do Sistema Multibiométrico da Polícia Federal e demanda a execução de um conjunto de atividades especializadas, voltadas ao monitoramento, suporte técnico e correção de seus componentes críticos. As principais tarefas a serem contempladas no escopo da contratação incluem:

6.4.6.1. Execução de serviços de manutenção preventiva e acompanhamento técnico de manutenções corretivas, com vistas a garantir a estabilidade, disponibilidade e desempenho do sistema como um todo.

6.4.6.2. Apoio à administração de rotinas de backup, mediante acompanhamento do armazenamento e orientação técnica quanto à execução e à validação dos procedimentos de

backup, visando assegurar a integridade e a recuperação dos dados biométricos e demais informações sensíveis.

6.4.6.3. Suporte técnico especializado na administração e gerenciamento do banco de dados do sistema, garantindo sua disponibilidade, segurança, integridade e desempenho.

6.4.6.4. Gerenciamento e monitoramento dos serviços de workflow e dos mecanismos de comparação biométrica (comparadores), com atuação proativa no balanceamento de cargas e na mitigação de eventuais gargalos de desempenho.

6.4.6.5. Sustentação das aplicações integrantes do ecossistema ABIS, assegurando sua operacionalidade contínua.

6.4.6.6. Gerenciamento e suporte nas ferramentas de geração de relatórios e estatísticas, com foco na manutenção da consistência e acessibilidade das informações estratégicas geradas pelo sistema.

6.4.6.7. Acompanhamento e análise das ferramentas de segurança da informação utilizadas pelo sistema, com a proposição de boas práticas e medidas preventivas, de modo a garantir a confidencialidade, integridade e disponibilidade das informações processadas.

6.4.6.8. Monitoramento da comunicação entre servidores e aplicações, com ações proativas voltadas à identificação de falhas, gargalos ou vulnerabilidades, bem como à proposição de melhorias técnicas.

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 foram definidos após diálogo com as empresas do setor em Audiência Pública realizada em 27 de novembro de 2025. A síntese desses requisitos está contida no Cronograma Físico Financeiro presente no Anexo VII deste Estudo Técnico Preliminar.

6.5.3. Na execução dos serviços deverão ser observados os seguintes prazos:

6.5.3.1. O Grau de Prioridade **Menor**: Funções não essenciais do sistema estão afetadas. Poucos usuários estão impactados. O problema implica em perda parcial de funcionalidades não críticas para a produção.

6.5.3.2. O Grau de Prioridade **Maior**: A capacidade de produção do sistema se encontra reduzida, alguns usuários são afetados. A situação está causando um impacto significativo na produtividade e operações dos clientes.

6.5.3.3. O Grau de Prioridade **Crítico**: O Sistema está indisponível, a maioria dos usuários está afetada. Uma oudas funcionalidades principais está inoperante. Ocorreu um problema muito grave que afeta severamente a produção da Polícia Federal.

| Classificação do Incidente | Prazo de registro e emissão de número de chamado | Prazo máximo de resolução de problema |
|---|---|---|
| Crítico | 2 horas corridas | 24 horas corridas |
| Maior | 4 horas úteis | 48 horas úteis |
| Menor | 6 horas úteis | 80 horas úteis |

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 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 com a participação da Contratada;

6.8.1.2. Não deve haver restrição à extração ou exportação direta dos dados para outros gerenciadores de banco, pelo menos para Oracle Database Server, Microsoft SQL Server PostgreSQL e MySQL Server, devendo a eventual conversão dos dados ser realizada com a participação da Contratada;

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:

6.9.1.1. Assinatura do contrato;

6.9.1.2. Realização de Projeto Executivo;

6.9.1.3. Instalação e Configuração dos Ambientes de Produção, Homologação, Treinamento e Testes. Os Ambientes de Homologação, Treinamento e Testes devem possuir capacidade de armazenamento de, no mínimo, um milhão de registros;

6.9.1.4. Migração e Deduplicação de dados biométricos;

6.9.1.5. Instalação e Configuração de Softwares Clientes;

6.9.1.6. 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:

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

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

6.10.1.3. 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.

6.11.2. O atestado deverá ser emitido por instituição de direito público ou privado, nacional ou estrangeira, que comprove a implantação de:

6.11.2.1. Sistema de identificação biométrica com base de dados de fragmentos de impressões digitais igual ou superior a 300 mil fragmentos de impressões digitais, operando pesquisas LT/TP em uma base de dados de registros decadactilares igual ou superior a 40 milhões de registros de Pessoas;

6.11.2.2. Sistema de identificação biométrica com base de dados de registros decadactilares igual ou superior a 40 milhões de registros de Pessoas no comparador da solução;

6.11.2.3. Sistema de reconhecimento facial, integrado ao papiloscópico, com solução de comparação combinada, utilizando fusão de scores de forma nativa, operando em uma base de dados de registros de imagens faciais igual ou superior a 40 milhões de registros;

6.11.3. Não será aceito o somatório das quantidades indicadas nos atestados de capacidade técnica por item, caso a empresa presente mais de um documento.

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 o 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 nº 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 nº 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)**

Não se aplica a essa contratação.

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

Não se aplica a essa contratação.

6.19. **Da exigência de carta de solidariedade**

Não se aplica a essa contratação.

6.20. **Subcontratação**

6.20.1. Permite-se a subcontratação para fornecimento e suporte de componentes de infraestrutura considerados padrão de mercado, tais como hardware, sistemas gerenciadores de banco de dados (SGBD), sistemas operacionais, plataformas de virtualização e kits de desenvolvimento de software (SDK). Essa autorização visa assegurar que a solução ABIS seja implementada com tecnologias consolidadas, certificadas e aderentes às melhores práticas do mercado, garantindo escalabilidade e continuidade operacional.

6.20.2. Outros itens podem ser discutidos no projeto executivo.

6.20.3. Fica vedada a subcontratação, total ou parcial, do objeto principal relativo ao sistema ABIS incluindo, mas não se limitando a:

a) Desenvolvimento e manutenção do software principal da solução ABIS;
b) Projeto Executivo e levantamento de requisitos;
c) Migração e deduplicação de dados;
d) Serviços de comparação biométrica (ABIS central) e manutenção evolutiva/corretiva.

6.20.4. A contratada permanecerá integralmente responsável pela entrega completa da solução, pelo cumprimento dos níveis de serviço (SLA), pela segurança da informação e pela interoperabilidade dos componentes, devendo formalizar os instrumentos de subcontratação que assegurem rastreabilidade, conformidade técnica e atendimento às exigências contratuais (incluindo certificações quando aplicáveis).

6.21. Por se tratar de contratação de serviços de grande complexidade técnica e com o objetivo de se garantir o atendimento aos requisitos técnicos exigidos e ampliar a competitividade, será admitida a participação de consórcios. A responsabilidade das empresas consorciadas será solidária pelas obrigações do consórcio, nas etapas de licitação e durante a vigência do contrato.

6.22. **Da verificação de amostra do objeto**

6.22.1. 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.

6.23. **Requisitos de garantia da contratação**

6.23.1. 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.

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

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

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

## 7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS

7.1. Itens previstos para atendimento da Demanda:

| Item | Descrição | Quantidade |
|---|---|---|
| Item 1 | Projeto Executivo | 01 unidade |
| Item 2 | Customização para Atender Requisitos | 01 unidade |
| Item 3 | Serviço de Instalação | 01 unidade |
| Item 4 | Serviço de Migração e Deduplicação de dados | 01 unidade |
| Item 5 | Serviço de Capacitação dos servidores da CONTRATANTE | 01 unidade |
| Item 6 | Serviço de Comparação Biométrica (ABIS) com capacidade para 277 milhões de pessoas e Manutenção do Sistema | XX |

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: 219.367.247;

7.2.1.2. Acumulado de brasileiros mortos entre 1996 e 2035: 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 e com entrada até 2035: 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. Quantidade de Estações de Trabalho Pericial

7.2.2.1. Número está vinculado ao quantitativo de postos ocupados de Papiloscopistas Policiais Federais (537 postos).

7.2.3. Quantidade de Estações de Cadastramento e de Dispositivos Móveis

7.2.3.1. O quantitativo baseia-se na atualização 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 | 5 | 5 |
| SR/PF/AL | 9 | 6 | 10 | 15 |
| SR/PF/AM | 11 | 3 | 11 | 5 |
| SR/PF/AP | 5 | 5 | 6 | 4 |
| SR/PF/BA | 10 | 9 | 9 | 6 |
| SR/PF/CE | 5 | 4 | 6 | 6 |
| SR/PF/DF | 6 | 3 | 6 | 3 |
| SR/PF/ES | 5 | 5 | 5 | 3 |
| SR/PF/GO | 5 | 5 | 4 | 4 |
| SR/PF/MA | 4 | 5 | 5 | 5 |
| SR/PF/MG | 43 | 25 | 44 | 69 |
| SR/PF/MS | 10 | 16 | 10 | 12 |
| SR/PF/MT | 9 | 7 | 7 | 7 |
| SR/PF/PA | 9 | 8 | 15 | 12 |
| SR/PF/PB | 6 | 3 | 6 | 4 |
| SR/PF/PE | 7 | 5 | 8 | 5 |
| SR/PF/PI | 12 | 5 | 7 | 5 |
| SR/PF/PR | 15 | 13 | 18 | 15 |
| SR/PF/RJ | 20 | 7 | 20 | 7 |
| SR/PF/RN | 6 | 4 | 6 | 4 |
| SR/PF/RO | 9 | 3 | 5 | 3 |
| SR/PF/RR | 16 | 5 | 14 | 15 |
| SR/PF/RS | 18 | 16 | 19 | 15 |
| SR/PF/SC | 15 | 9 | 17 | 9 |
| SR/PF/SE | 3 | 4 | 8 | 4 |
| SR/PF/SP | 50 | 39 | 53 | 39 |
| SR/PF/TO | 7 | 3 | 11 | 9 |
| INI/DPA/PF e outros Órgãos Centrais | 20 | 45 | 20 | 45 |

| | | | | |
|---|---|---|---|---|
| TOTAL | 340 | 267 | 355 | 335 |

8. **LEVANTAMENTO DE SOLUÇÕES**

8.1. **Solução 1: Software Público**

8.1.1. Regido pela Portaria STI/MP nº 46, de 28/09/2016 (alterada pela Portaria SGD/ME nº 3, de 27/06/2019), o Portal de Software Público Brasileiro oferece soluções em software livre que buscam atender boa parte das 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.

8.2. **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.

8.3. **Solução 3: Ampliação da Solução Implantada**

8.3.1. Essa solução busca a ampliação de capacidade do sistema adquirido através do contrato 01/2021 - DTI/PF.

8.4. **Solução 4: Contratação com Empresa Pública**

8.4.1. Essa solução busca a contratação de empresa pública que desenvolva e forneça sistemas ABIS ou que subcontrate o fornecimento de sistemas ABIS. 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).

8.5. **Solução 5: Aquisição de Software**

8.5.1. Essa solução é definida pela contratação por aquisição de licenças por núcleo de processamento e por licenças de sistemas clientes. Nessa solução, hardware e serviços, como também a manutenção, são adquiridos separadamente. Esta foi a solução implementada na contratação 01/2021 - DTI/PF.

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 a solução deverá 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: Serviço Integrado**

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

9. **ANÁLISE COMPARATIVA DAS SOLUÇÕES**

| **Requisito** | **Soluções** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? | Não | Não | Não | Sim | Sim | Sim | Sim |
| A Solução está disponível no Portal do Software Público Brasileiro? | Não | Não | Não | Não | Não | Não | Não |
| A Solução é composta por software livre ou software público? | Sim | Sim | Não | Não | Não | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag e ePWG? | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica |
| A Solução é aderente às regulamentações da ICP-Brasil? | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica |
| A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica | Não se aplica |

10. **REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS**

10.1. **Solução 1: Software Público**

10.1.1. Nas pesquisas realizadas no Catálogo de Software Público, não foram encontradas soluções que atendessem as necessidades desta contratação.

10.1.2. Esses softwares não se encaixam nas exigências de capacidade, requisitos funcionais e acurácia, além da necessidade de suporte ou desenvolvimento complementar.

10.2. **Solução 2: Software Livre**

10.2.1. Nas pesquisas realizadas por Softwares Livres, não foram encontradas soluções que atendessem as necessidades desta contratação.

10.2.2. Esses softwares não se encaixam nas exigências de capacidade, requisitos funcionais e acurácia, além da necessidade de suporte ou desenvolvimento complementar.

10.3. **Solução 3: Ampliação da Solução Implantada**

10.3.1. O contrato 01/2021 - DTI/PF não prevê a possibilidade de ampliação da solução implantada para a capacidade necessária.

10.3.2. Grande probabilidade de descompasso nas compras de hardware para acompanhar o cronograma de expansão.

10.3.3. A solução implantada não atende aos novos requisitos negociais imprescindíveis, notadamente os de ACE-V, acurácia, mudanças de Workflow, armazenamento de SMT, atualização de campos de preenchimento, interface Web, biometria neonatal, entre outras.

10.4. **Solução 4: Contratação com Empresa Pública**

10.4.1. Não foi encontrada contratação com os requisitos semelhantes a essa aquisição.

10.5. **Solução 5: Aquisição de Software**

10.5.1. A aquisição do hardware de forma separada traz dois riscos: adquirir uma quantidade abaixo do necessário ou, ao contrário, superestimar a demanda. Além disso, comprar o hardware antes do software ABIS é inviável, pois o dimensionamento do hardware depende diretamente dos requisitos do sistema. Por outro lado, se a compra do hardware ocorrer apenas após a contratação do software, haverá atraso na implantação do sistema e risco de inviabilidade orçamentária.

10.5.2. 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.

10.5.3. A falta de hardware para a realização das inserções biométricas previstas é um problema do sistema ABIS atual e impacta o cumprimento de acordos de cooperação firmados. O Instituto Nacional de Identificação possui uma demanda de inserções biométricas represada desde abril de 2024 em função da falta de hardware.

10.5.4. Dificuldade de integração de crescimento do sistema ABIS com aquisições escalonadas de hardware.

10.5.5. Descompasso entre a manutenção de software e manutenção de hardware, complexificando e atrasando o acionamento da garantia. Problemas de comunicação entre fornecedores, gerando dificuldade de responsabilização e atraso na resolução de problemas.

10.6. **Solução 6: Aquisição Integrada**

10.6.1. A aquisição do hardware através de um fornecedor de software ABIS restringe a competitividade da aquisição do hardware.

10.6.2. Dado o horizonte da contratação, não é interessante adquirir hardware em função da obsolescência tecnológica.

10.6.3. Adquirir o hardware e o software implica dedicar recursos humanos e financeiros para manter a aquisição após a finalização do contrato.

11. **ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

| Solução | Estimativa (R$) |
|---|---|
| Solução 1: Software Público | SOLUÇÃO INVIÁVEL |
| Solução 2: Software Livre | SOLUÇÃO INVIÁVEL |
| Solução 3: Ampliação da Solução Implantada | SOLUÇÃO INVIÁVEL |
| Solução 4: Contratação com Empresa Pública | SOLUÇÃO INVIÁVEL |
| Solução 5: Aquisição de Software | SOLUÇÃO INVIÁVEL |
| Solução 6: Aquisição Integrada | SOLUÇÃO INVIÁVEL |
| Solução 7: Serviço Integrado | R$ XX |

12. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

O serviço de solução integrada é composto por hardware, software e serviços, fornecidos pela empresa dentro das dependências da Polícia Federal.

Ressalta-se que, após o encerramento do contrato, a infraestrutura de hardware e software pertence à contratada, que apenas disponibiliza e cobra pelo acesso aos serviços.

O Serviço Integrado será composto por cinco itens:

a) Projeto Executivo;
b) Serviço de Instalação Nacional dos Sistemas Clientes;
c) Serviço de Migração e Deduplicação de dados;
d) Serviço de Capacitação dos servidores da CONTRATANTE;
e) Serviço de Comparação Biométrica (ABIS) com capacidade para 277 milhões de pessoas e Manutenção do Sistema.

Após análises e obtenção das informações da Consulta Pública nº 19/2025, a Equipe de Planejamento da Contratação concluiu que a alternativa que melhor se adequa aos interesses públicos é a Solução 7 Serviço Integrado.

13. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

| Item | Descrição | Quantidade | Valor Unit. | Valor Total |
|---|---|---|---|---|
| Item 1 | Projeto Executivo | 01 unidade | R$ XX | R$ XX |
| Item 2 | Customização para Atender Requisitos | 01 unidade | R$ XX | R$ XX |
| Item 3 | Serviço de Instalação Nacional dos Sistemas Clientes | 01 unidade | R$ XX | R$ XX |
| Item 4 | Serviço de Migração e Deduplicação de dados | 01 unidade | R$ XX | R$ XX |
| Item 5 | Serviço de Capacitação dos servidores da CONTRATANTE | 01 unidade | R$ XX | R$ XX |
| Item 6 | Serviço de Comparação Biométrica (ABIS) com capacidade para 277 milhões de pessoas e Manutenção do Sistema | XX | R$ XX | R$ XX |

14. **JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO**
15. **BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO**
16. **PROVIDÊNCIAS A SEREM ADOTADAS**
17. **DECLARAÇÃO DE VIABILIDADE**
18. **RESPONSÁVEIS**

**ANEXO I**

**CONTEÚDO MÍNIMO DO PLANO DE AULA - CURSO DE CAPACITAÇÃO DE OPERADOR**

1. **MÓDULO PESSOA (40 horas)**
    - 1.1. **Introdução ao ABIS**. Visão geral do sistema e suas aplicações, ferramentas, capacidades e desempenhos.
    - 1.2. **Fluxos do sistema.** Visão geral sobre os fluxos de trabalho que os dossiês podem percorrer para inserção de PESSOAS.
    - 1.3. **Ferramenta de captura de dados.**
        - 1.3.1. Tipos de inclusão (ficha digitalizada, individuais, NIST, somente foto, scanner, etc.);
        - 1.3.2. Tratamento de resolução de imagem na ferramenta (contagem de cristas, contagem de mm ou polegadas, alteração somente de metadados);
        - 1.3.3. Inserções para diferentes coletas (somente dedos, dedos e palmas, somente roladas, roladas e batidas e etc.) com ou sem foto;
        - 1.3.4. Dados do fluxo: número de candidatos, prioridade, fluxo passando por UL etc.
    - 1.4. **Ferramenta de visualização de pesquisas pendentes.**
        - 1.4.1. Controle de qualidade e suas funcionalidades
        - 1.4.2. Realização de Pesquisas e ACE-V:
            - 1.4.2.1. Verificação de PESSOA/PESSOA;
            - 1.4.2.2. Validação de PESSOA/PESSOA;
            - 1.4.2.3. Consistência de PESSOA/PESSOA;
            - 1.4.2.4. Verificação de PESSOA/Latente Finger ou Face;
            - 1.4.2.5. Validação de PESSOA/Latente Finger ou Face;
            - 1.4.2.6. Consistência de PESSOA/Latente Finger ou Face;
        - 1.4.3. Controle de ID;
        - 1.4.4. Confirmação de deleção;
        - 1.4.5. Verificação de status, histórico e outros metadados do dossiê;
        - 1.4.6. Ferramenta gráfico;
        - 1.4.7. Relatórios de correspondência, mapas de minúcias, histórico de modificações; (minúcias e melhorias gráficas) e etc.
    - 1.5. **Ferramenta de consulta e recuperação de dados visando consulta, alteração ou relançamento.**
        - 1.5.1. Buscas pelos diferentes campos – incluindo consulta onomástica;
        - 1.5.2. Impressão de uma ficha;
        - 1.5.3. Exportação de uma ficha – NIST e outros;
        - 1.5.4. Relançamento da ficha em uma nova busca – aberta, fechada (ou interabis), versus TP ou UL;
        - 1.5.5. Exclusão de uma ficha;
        - 1.5.6. Controle de qualidade *a posteriori*.
    - 1.6. **Ferramenta de confronto ou recuperação de serviços realizados.**
        - 1.6.1. Confronto entre impressões e atentes externas ao ABIS;
        - 1.6.2. Confronto entre impressões e latentes externas ao ABIS com interna e vice-versa;
        - 1.6.3. Recuperar serviços já realizados como PESSOA/PESSOA ou PESSOA/LATENTE.
    - 1.7. **Gerenciador de listas.** Criação de listas para confrontos fechados.
    - 1.8. **Customizações da ferramenta.** Alterações de cores, dimensões e disposição dos elementos gráficos na tela etc.
    - 1.9. **Resoluções de problemas a nível de usuário.** Dossiês represados, licenças, serviços etc.
2. **MÓDULO LATENTE (40 horas)**
    - 2.1. **Fluxos do sistema.** Visão geral sobre os fluxos de trabalho que os dossiês podem percorrer para inserção de LATENTES.
    - 2.2. **Regras de codificação.** Como o sistema enxerga as minúcias? O operador precisa entender para marcar como a máquina marca.
    - 2.3. **Ferramenta de captura de dados.**
    - 2.4. **Caso Pericial:**
        - 2.4.1. Criação e alteração de Caso Pericial;
        - 2.4.2. Criação e alteração de Evidência;

2.4.3. Criação e alteração de Latente – possíveis melhorias da imagem;
2.4.4. Criação e alteração de codificação e seus filtros;
2.4.5. Envios (aberta, fechada, interabis);
2.4.6. Pessoas excluídas do caso.

2.5. **Recuperação de casos:**
2.5.1. Alteração do caso;
2.5.2. Exportação do caso;
2.5.3. Estatísticas do caso;
2.5.4. Filtros – agência, número, número antigo, expert etc.

2.6. **Ferramenta de fluxo.**
2.7. **Realização de Pesquisas e ACE-V.**
2.8. **Verificação de LATENTE/PESSOA.**
2.9. **Validação de LATENTE/PESSOA.**
2.10. **Consistência de LATENTE/PESSOA.**
2.11. **Confirmação de deleção.**
2.12. **Verificação de status, histórico e outros metadados do dossiê.**
2.13. **Ferramenta gráfico.**
2.14. **Relatórios de correspondência, mapas de minúcias, histórico de modificações (minúcias e melhorias gráficas) e etc.**

3. **MÓDULO FACE (20 horas)**

3.1. **Caso Pericial.**
3.1.1. Criação e alteração de Caso Pericial;
3.1.2. Criação e alteração de Evidência;
3.1.3. Criação e alteração de Latente – possíveis melhorias da imagem;
3.1.4. Criação e alteração de codificação e seus filtros;
3.1.5. Envios (aberta, fechada, interabis);
3.1.6. Pessoas excluídas do caso;
3.1.7. Realização de Pesquisas e ACE-V.

3.2. **Conhecimento em regulação, leis e políticas ligadas ao uso de biometrias.**
3.3. **Risco de Vieses do Sistema.**
3.3.1. Falsos Positivos e Falsos Negativos;
3.3.2. Calibragem e Ajuste do Sistema;
3.3.3. Configuração para diferentes circunstâncias e riscos.

3.4. **Risco de Vieses do Operador.**
3.4.1. Superestimação da própria capacidade;
3.4.2. Dependência da tecnologia (score);
3.4.3. Pontos cegos;
3.4.4. Preconceito diversos, inclusive de raça.

3.5. **Consciência do Risco de Manipulação de Imagens.**
3.6. **Políticas de mitigação de riscos.**
3.7. **Compreensão dos documentos técnicos gerados e de sua aplicação.**
3.8. **Conhecimento de processos de governança de dados, incluindo coleta, armazenamento, integridade e rastreabilidade dos dados**.

4. **MÓDULO ESTAÇÃO DE COLETA E DISPOSITIVO DE AUTENTICAÇÃO (10 horas)**

4.1. **Estação de Coleta Fixa.**
4.1.1. Tipos de inclusão (ficha digitalizada, individuais, NIST, somente foto, scanner, etc.);
4.1.2. Inserções para diferentes coletas (somente dedos, dedos e palmas, somente roladas, roladas e batidas e etc.) com ou sem foto.
4.1.3. Dados do fluxo: número de candidatos, prioridade, fluxo passando por UL etc.

4.2. **Conexão com o ABIS/PF.**
4.3. **Dispositivo de Autenticação Móvel.**
4.4. **Resoluções de problemas a nível de usuário.** Dossiês represados, licenças, serviços etc.

**ANEXO II**

**CONTEÚDO MÍNIMO DO PLANO DE AULA - CURSO DE CAPACITAÇÃO DE ADMINISTRADOR**

1. Apresentação da arquitetura;
2. Apresentação da configuração instalada;
3. Administração de rede;
4. Solução antivírus;
5. Aspectos de administração do SGBD (Sistema Gerenciador de Banco de Dados) relacionado com o sistema;
6. Backup e Solução Disaster Recovery (DR);
7. Verificação de backup e DR;
8. Tarefas diárias;
9. Ferramentas de Supervisão aplicativa do sistema;
10. Supervisão dos aplicativos Web;
11. Ferramenta de edição do fluxo do sistema;
12. Ferramenta de cadastramento e controle de usuários e unidades.
13. Módulos operacionais e administrativos do sistema implantado.
14. Instalação Física, Gerenciamentos e Monitoração;
15. Utilização do Software ou Interface de Gerenciamento;
16. Verificação e Isolamento de erros;
17. Reconfiguração do Sistema;
18. Procedimentos de Recuperação em caso de falha de componentes;
19. Atualização dos componentes de software e Firmware do sistema;
20. Configuração para operação dualizada ou de Alta Disponibilidade;
21. Configuração para operações de desastre e recuperação de dados.
22. Geração de relatórios para análise dos eventos registrados pelo sistema (LOGs, acessos de usuários, visualização de licenças, status do sistema etc.);
23. Importação e exportação de dados para outras bases de dados utilizando as ferramentas do sistema;
24. Exploração prática, em diversos cenários indicados pelos treinandos, das potencialidades do sistema.
25. Configurações de usuários, administradores, supervisores, estações de trabalho, criação e eliminação de senhas, criação de tabelas de privilégios por tipo de usuários etc.
26. Melhores práticas para geração das mídias gravadas, backup, recuperação de backups, e demais operações para extração e gravação das seções de trabalho.
27. Outros tópicos necessários para o pleno domínio da Plataforma de Storage e suas Integrações.

**ANEXO III**

**PLANO DE AÇÃO EDUCACIONAL**

**NOME DA AÇÃO EDUCACIONAL** (curso, treinamento, workshop, seminário etc.)

1. **JUSTIFICATIVA** (Conjunto de informações e análises que lastreiam a realização da ação educacional):
2. **OBJETIVOS** (estabelecimento dos resultados esperados com a realização da ação educacional):
3. **PÚBLICO-ALVO** (a quem se destina a ação educacional):
4. **CRITÉRIO DE PARTICIPAÇÃO** (fixação de pré-requisitos aos alunos, cuja existência é necessária para que a ação educacional alcance os objetivos estabelecidos na carga-horária fixada):
5. **ORGANIZAÇÃO**

**5.1. Metodologia** (Estabelecimento da metodologia adequada à construção do conhecimento e ao alcance dos objetivos estabelecidos, dentre diversas estratégias - aulas expositivas dialogadas, apresentação de slides, conceituação teórica ilustrada por situações reais, estudos de casos, dinâmicas de grupo, aulas práticas, visitas técnicas supervisionadas, realização de trabalhos individuais e coletivos, apresentações etc.).

**5.2. Duração**

**5.2.1.** O curso será realizado no período XXXXX, com carga horária total de XXXX (XXXXXXX) horas-aula, distribuídas em XXXX (XXXX) dias letivos, com X (XXX) horas-aula de atividades diárias.

**5.3. Distribuição do tempo**

**5.3.1. Teórica ..... XX h/a**

**5.3.2. Prática ..... XX h/a**

**5.3.3. Total ..... XX h/a**

**5.4. Grade Curricular** (Disciplina ou conjunto de disciplinas que serão ministradas)

| DISCIPLINA | EMENTA | CARGA-HORÁRIA |
|---|---|---|
| | | |
| | | |

**5.5. Grade Horária** (Distribuição da carga-horária da(s) disciplina(s) pelo período estabelecido para a realização da ação educacional)

| GRADE HORÁRIA | | | | |
|---|---|---|---|---|
| DATA | HORÁRIO | | | |
| | 08h00 / 09h00 | 09h10 / 10h10 | (...) | (...) |
| | DISCIPLINA/PROFESSOR | | | |
| | | | | |
| | | | | |

**5.6. Frequência** (Estabelecimento dos critérios de participação e aproveitamento da ação educacional. Exemplo: Será conferido certificado de aproveitamento aos participantes que obtiverem frequência mínima de XXXXX% da carga horária total da ação educacional)

**6. EQUIPE TÉCNICO-PEDAGÓGICA**

**7.DISPOSIÇÕES DIVERSAS**

7.1. O curso será realizado (localidade)
7.2. Os conteúdos programáticos serão ministrados de conformidade com o Plano de Disciplina elaborado pelos docentes ou prestador de serviço.
7.3. Os casos omissos serão dirimidos pelo INI/DPA/PF e pela DTI/PF.

_____
CONTRATADO

Aprovo,
Brasília/DF, ___ de _____ de 20__

_____
CONTRATANTE

**ANEXO IV**

**AVALIAÇÃO DE REAÇÃO E SATISFAÇÃO DA AÇÃO EDUCACIONAL**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| ASPECTO AVALIADO | ITEM | QUESITO | CRITÉRIOS DE AVALIAÇÃO | | | | |
| | | | EXCE LENTE | BOM | REGULAR | RUIM | PÉSSI MO |
| ESTRUTURA DO CURSO | 1 | O curso apresenta um plano de ensino bem definido e estruturado? | | | | | |
| | 2 | Os conteúdos abordados foram adequados para a formação técnica do instrutor (multiplicador) do sistema ABIS? | | | | | |
| | 3 | O curso abordou de forma satisfatória os aspectos teóricos e práticos do sistema? | | | | | |
| | 4 | Os exercícios práticos foram suficientes e relevantes na assimilação do conteúdo? | | | | | |
| | 5 | A carga horária é adequada para o aprendizado completo da tecnologia ABIS? | | | | | |
| | 6 | As instalações e os equipamentos atenderam às necessidades do treinamento? | | | | | |
| CONTEÚDO TÉCNICO E APLICABILIDADE | 7 | Os conceitos técnicos sobre biometria e funcionamento do ABIS foram bem explicados? | | | | | |
| | 8 | O curso cobre conceitos fundamentais e avançados de biometria (impressão digital, reconhecimento facial)? | | | | | |
| | 9 | Ensina a operação prática do sistema ABIS, incluindo captura, processamento, edição, análise e comparação de dados biométricos? | | | | | |
| | 10 | Apresenta cenários reais de aplicação, como registro, pesquisa e identificação civil e criminal? O material didático (cadernos didáticos, manuais, apresentações, textos etc.) disponibilizado auxiliou no processo de aprendizagem? | | | | | |
| | 11 | Apresenta cenários reais de aplicação, como registro de casos periciais papiloscópicos e faciais, pesquisa e solução de crimes? | | | | | |
| | 12 | Apresenta cenários reais para a utilização de ferramentas, filtros e edição avançadas em evidências modelo? | | | | | |
| | 13 | Você se sente preparado para utilizar o sistema ABIS, estando apto a elaborar treinamentos de utilização do Sistema ABIS para operadores? | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| EXECUÇÃO - METODOLOGIA DE ENSINO | 14 | As aulas combinam teoria e prática de maneira equilibrada? | | | | | |
| | 15 | Há demonstrações ou simulações reais do uso do sistema ABIS? | | | | | |
| | 16 | Os alunos têm acesso ao ambiente de treinamento com acesso a todas as funcionalidades necessárias para o aprendizado? | | | | | |
| | 17 | Disponibiliza materiais de apoio, como apostilas, vídeos e exercícios? | | | | | |
| QUALIFICAÇÃO DOS INSTRUTORES | 18 | O instrutor demonstrou didática eficiente e experiência prática sobre o sistema ABIS? | | | | | |
| | 19 | O instrutor utilizou exemplos práticos para facilitar o aprendizado? | | | | | |
| | 20 | O instrutor respondeu de forma satisfatória às dúvidas dos participantes? | | | | | |
| RECURSOS E INFRAESTRUTURA (LOGISTICA) | 21 | O curso oferece acesso a plataformas reais ou simuladas do sistema ABIS? | | | | | |
| | 22 | O acesso ao sistema ABIS durante o treinamento foi eficiente e sem problemas técnicos? | | | | | |
| AVALIAÇÃO E CERTIFICAÇÃO | 23 | Há avaliações práticas para medir o desempenho dos alunos? | | | | | |
| | | | | | | | |

**ANEXO V**

**PAUTA DE CONTROLE DE FREQUÊNCIA**

| CONTROLE DE FREQUÊNCIA - ALUNOS | |
|---|---|
| **AÇÃO EDUCACIONAL:** | |
| **PAUTA REFERENTE AO DIA:** | **PERÍODO*: (MANHÃ/TARDE/NOITE)** |

| NOME COMPLETO | ASSINATURA |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

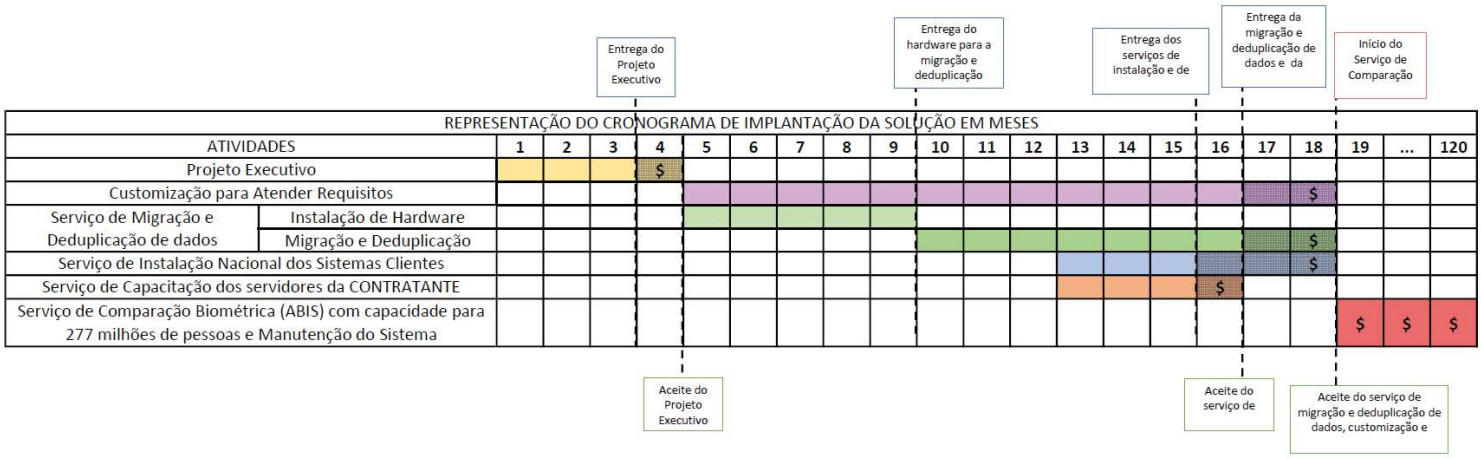
**ANEXO VI**

**LISTA MÍNIMA DE APIS A SEREM DISPONIBILIZADAS**

1. Inserção de Registro no ABIS: Objetivo: Inserir novo registro com dados identificativos e biométricos. Entrada esperada: Dados identificativos, imagens faciais (base64, fotografias frontal, diagonal e laterais), imagens de impressões digitais (10 roladas, 4 batidas), formatos JPG/PNG. Saída mínima: Aceito e ID de fluxo com posterior envio de Identificador do novo registro ou não aceito.
2. Recuperação de Dados por Identificador de Pessoa: Objetivo: Retornar todos os registros, dados identificativos e biometrias vinculados. Entrada mínima: Identificador numérico da pessoa. Saída mínima: JSON com dados da pessoa.
3. Recuperação de Registro Específico: Objetivo: Retornar dados de um registro específico. Entrada mínima: Identificador de pessoa. Saída mínima: JSON com dados do registro correspondente.
4. Consulta de Status do Fluxo de Trabalho: Objetivo: Consultar status de um workflow no sistema. Entrada mínima: Identificador de fluxo. Saída mínima: Status do fluxo.
5. Comparação com Base de Latentes (TP/UL): Objetivo: Comparar impressões digitais com banco de latentes não resolvidos. Entrada mínima: De 1 a 10 impressões digitais. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
6. Comparação de Palmares com Latentes (PP/UP): Objetivo: Comparar impressão palmar com banco de latentes não resolvidos. Entrada mínima: Impressão palmar. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
7. Comparação de Latente com Base de Pessoas (LTTP/LPTP): Objetivo: Verificar correspondência de impressão latente com banco de pessoas. Entrada mínima: Fragmento de impressão digital ou palmar. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
8. Comparação de Latente com Base de Pessoas (LTTP/LPTP): Objetivo: Verificar correspondência de impressão latente com banco de pessoas. Entrada mínima: Fragmento de impressão palmar. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
9. Comparação de Latente com Base de Latentes (LTUL/LPUP): Objetivo: Comparar impressão latente com outras latentes não resolvidas. Entrada mínima: Fragmento de impressão digital ou palmar. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
10. Comparação de Latente com Base de Latentes (LTUL/LPUP): Objetivo: Comparar impressão latente com outras latentes não resolvidas. Entrada mínima: Fragmento de impressão palmar. Saída mínima: Aceito com ID de fluxo com posterior envio de correspondência ou não aceito.
11. Exclusão de Pessoa: Objetivo: Executar fluxo de exclusão de pessoa. Entrada mínima: Identificador de pessoa. Saída mínima: Aceito ou não aceito.
12. Exclusão de Registro: Objetivo: Executar exclusão de registro específico. Entrada mínima: Identificador de registro. Saída mínima: Aceito ou não aceito.
13. Localização de Pessoa por Filtros: Objetivo: Buscar pessoa usando múltiplos filtros identificativos. Entrada mínima: Dados de pesquisa. Saída mínima: JSON com identificadores compatíveis.
14. Atualização de Dados por Identificador: Objetivo: Atualizar dados identificativos de pessoa cadastrada. Entrada mínima: Dados de atualização e identificador de registro. Saída mínima: Aceito ou não aceito.

**ANEXO VII**

**CRONOGRAMA DE IMPLANTAÇÃO**




| REPRESENTAÇÃO DO CRONOGRAMA DE IMPLANTAÇÃO DA SOLUÇÃO EM MESES | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ATIVIDADES | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | ... | 120 |
| Projeto Executivo | | | | | $ | | | | | | | | | | | | | | | | | |
| Customização para Atender Requisitos | | | | | | | | | | | | | | | | | | | $ | | | |
| Serviço de Migração e Deduplicação de dados | Instalação de Hardware | | | | | | | | | | | | | | | | | | | | | |
| | Migração e Deduplicação | | | | | | | | | | | | | | | | | | $ | | | |
| Serviço de Instalação Nacional dos Sistemas Clientes | | | | | | | | | | | | | | | | | | | $ | | | |
| Serviço de Capacitação dos servidores da CONTRATANTE | | | | | | | | | | | | | | | | | $ | | | | | |
| Serviço de Comparação Biométrica (ABIS) com capacidade para 277 milhões de pessoas e Manutenção do Sistema | | | | | | | | | | | | | | | | | | | | $ | $ | $ |