APÊNDICE A - ESPECIFICAÇÃO TÉCNICA

O escopo de contratação incluirá dois componentes para a implementação do Sistema Automatizado de Identificação Biométrica (ABIS): o motor biométrico, responsável pelo processamento das características biométricas dos cidadãos, e o módulo de tratamento de inconsistências, que garantirá a resolução de conflitos durante o processo de deduplicação, assegurando a unicidade e precisão dos registros.

Essa solução será instalada nos data centers da Dataprev, em conformidade com os parâmetros de infraestrutura descritos no item 4 desse anexo, garantindo assim a compatibilidade e eficiência operacional do sistema.

1. MOTOR BIOMÉTRICO

O motor biométrico é o componente central do ABIS, responsável por processar as características biométricas de cada cidadão. Deve ser capaz de realizar a inserção com garantia de unicidade biométrica, exclusão lógica, alteração e comparação destes dados, seja a identificação (1:N) ou a verificação (1:1). As operações biométricas devem ser realizadas em modalidades como impressões digitais e reconhecimento facial. Deve ainda permitir a realização de consultas a partir de dados biométricos e a realização de processos de verificação de vivacidade (liveness).

1.1. **Volumetria**:

A solução ABIS deve ser capaz de:

1.1.1. Realizar operações de identificação **1:n**, conforme a seguinte estimativa:

Biometria	Captura	Ano 0 - 2024 (milhões)	Ano 1 - 2025 (milhões)	Ano 2 - 2026 (milhões)	Ano 3 - 2027 (milhões)	Ano 4 - 2028 (milhões)	Ano 5 - 2029 (milhões)	Total (milhões)
Imp. digital + Facial	rolada +mugshot	20	36	42	42	36	24	200

(Estimativa de operação de identificação 1:n)

1.1.2. Realizar operações de identificação **1:1**. Para fins informativos, a volumetria dos serviços atualmente executados pela Dataprev passíveis de validação biométrica esta em torno de 94 (noventa e quatro) milhões).

1.1.3. As estimativas de volumetria de 1:n e 1:1 acima identificadas foram elaboradas com base na Portaria SGD/MDI nº 6.618, de 25 de setembro de 2024, e nos serviços atualmente executados pela Dataprev passíveis de validação biométrica, respectivamente, para fins de levantamento dos aspectos de infraestrutura.

1.1.3.1. Eventual superação das estimativas, por si só, não será causa de concessão de reequilíbrio econômico-financeiro, uma vez que os pagamentos serão efetuados de acordo com o quantitativo de dados biométricos inseridos na base.

1.1.4. Cada registro biométrico de um indivíduo único (*template*) deve ser, minimamente, composto por:

1.1.4.1. até 10 impressões digitais;

1.1.4.2. fotografia do tipo de registro de identificação Civil;

1.1.5. Permitir escalabilidade, ou seja, os componentes que realizam funções computacionais intensivas (Banco de Dados, Matchers Biométricos, etc) deverão permitir o aumento da capacidade de atendimento de requisições através da adição de hardware (de forma horizontal e vertical), sem impactos no funcionamento e na configuração do Solução ABIS.

1.1.6. O processo de vivacidade (liveness) tem como objetivo garantir que a característica biométrica capturada é proveniente de um ser humano vivo e não de uma falsificação ou apresentação de uma característica biométrica artificial. Deve atender no mínimo os requisitos abaixo:

I - Para transações de baixo risco: Face liveness 2D passivo, em conformidade com padrão ISO 30107-3 Level 1, sem certificação, apto para receber a certificação iBeta Level 1.

II - Para transações de médio a alto risco: Face liveness 2D passivo em conformidade com os padrões ISO 30107-3 Level 1, ISO 30107-3 Level 2 e certificação NIST FATE evaluation of passive facial presentation attack detection (PAD).

III - Para transações alto risco: Face liveness 3D ativo para transações de alto risco em conformidade com os padrões ISO 30107-3 Level 1 e ISO 30107-3 Level 2.

1.2. **Tempo de Resposta**

1.2.1. Realizar operações de identificação (1:N) em menos de 5 dias;

1.2.2. Realizar operação de verificação (1:) em menos de 1 segundo;

1.2.3. Ter o tempo de resposta para uma operação com complexidade máxima linear em função da quantidade de registros na base;

1.2.4. Garantir que a carga máxima prevista para uma configuração de hardware execute sem degradação no tempo de resposta das operações de identificação;

1.2.5. Evitar colapsos e quedas do Sistema em picos de transações. O Sistema deverá permitir a administração da fila de transações.

1.3. **Padrões Técnicos Biométricos**

1.3.1. Os dados da impressão digital devem atender aos padrões NIST Fingerprint Image Quality (NFIQ) 2, em acordo com a ISO/IEC 29794-4;

1.3.2. Os dados da face serão submetidos ao padrão estabelecido pelo Documento 9303, da International Civil Aviation Organization (ICAO), em acordo com a ISO/IEC 29794-5;

1.3.3. O algoritmo do motor biométrico deve atender aos parâmetros mínimos de interoperabilidade exigidos pelo NIST (compliance) para os algoritmos biométricos da solução, sendo certificado NIST MINEX III;

1.3.4. O algoritmo do motor biométrico deverá estar listado entre os padrões e testes mais recente do NIST, especificamente o Face Recognition Technology Evaluation (FRTE) 1:N para face e o MINEX III para impressões digitais.

1.4. **Acurácia**

1.4.1. O resultado da FNIR a um FPIR fixo de 0,001 deve ser 0,03 ou menos para o teste de Classe A de “Left Index” ou “Right Index”, realizado sobre um tamanho de banco de dados de 100.000, verificável no relatório final do teste de FpVTE (NIST.IR.8034);

1.4.2. O resultado da FNIR a um FPIR fixo de 0,001 deve ser 0,0033 ou menos para o teste “Identification Flats” Classe B, realizado sobre um tamanho de banco de dados de 3.000.000, verificável no relatório final do teste FpVTE (NIST.IR.8034);

1.4.3. O resultado da FNIR a um FPIR fixo de 0,001 deve ser 0,0095 ou menos para o teste “Ten-Finger Plain-to-Plain ” Classe C, realizado sobre um tamanho de banco de dados de 5.000.000, verificável no relatório final do teste FpVTE (NIST.IR.8034);

1.4.4. O resultado da FNIR a um FPIR fixo de 0,001 deve ser 0,0085 ou menos para o teste "Immigration visa-border", realizado sobre um tamanho de banco de dados de 1.600.000 assuntos para qualquer um de seus envios de algoritmos, verificável nos relatórios FRVT 1:N Identification (https://pages.nist.gov/frvt/html/frvt1N.html).

1.5. **Ambientes tecnológicos**

A solução ABIS deverá contar com três ambientes tecnológicos distintos para

garantir o correto desenvolvimento, teste e operação do sistema:

a) **Desenvolvimento**: Utilizado para a criação e aprimoramento de funcionalidades, o ambiente de desenvolvimento permitirá que as equipes técnicas trabalhem em novos recursos e ajustes da solução sem interferir nos ambientes de homologação e produção. Neste espaço, serão realizadas implementações iniciais, bem como os testes preliminares das funcionalidades desenvolvidas.

b) **Homologação**: Esse ambiente tem como função replicar o ambiente de produção o mais fielmente possível, sendo utilizado para a validação de funcionalidades antes de sua liberação definitiva. No ambiente de homologação, os testes finais de qualidade e desempenho serão realizados para garantir que os novos componentes ou atualizações estejam em conformidade com os requisitos operacionais antes de serem implementados no ambiente de produção.

c) **Produção**: O ambiente de produção será o espaço onde o ABIS estará plenamente operacional, processando os dados biométricos reais dos cidadãos e garantindo que o sistema funcione com alta disponibilidade e segurança. Todas as operações de deduplicação, consultas e manutenção dos registros serão executadas nesse ambiente, assegurando a eficiência e a integridade do sistema em escala nacional.

1.6. Requisitos tecnológicos obrigatórios

1.6.1. Integração e consumo das funcionalidades através do uso de APIs;

1.6.2. Comunicação com os serviços disponibilizados pela solução utilizando-se protocolos padronizados (*HTTP* e *JSON*, por exemplo);

1.6.3. Caso o fabricante, para atender a especificação, tenha de fornecer mais de um produto, será aceito a utilização de mais de uma console, desde que os sistemas sejam do mesmo fabricante, e com possibilidade de incluir licenciamento e instalação de uma console unificada, quando disponibilizada pelo fabricante sem ônus para a DATAPREV (aceita-se documentação):

1.6.3.1. A gerência da solução será composta por no mínimo 2 (Dois) Servidores de Gerenciamento Centralizado – poderão deverão ser instaladas duas gerências centralizadas em localidades e VLANs distintas, em dois dos Data Centers da DATAPREV, ambos funcionando em esquema *Disaster Recovery* (DR) de ativo/standby ou ativo/ativo;

1.6.3.2. A solução de gerência deve ter a seguinte configuração:

1.6.3.2.1. Uma das gerências deve ser primária (ativa);

1.6.3.2.2. Uma das gerências deve ser secundária (passiva);

1.6.3.2.3. Em caso de falha da gerência primária (ativa), automaticamente a secundária (passiva) deve assumir o gerenciamento centralizado da solução;

1.6.3.2.4. As configurações devem ser sincronizadas em tempo real entre a gerência primária (ativa) e a gerência secundário (passiva).

1.6.3.3. A console de gerenciamento deve estar acessível através do Navegador Web (Protocolos HTTP ou HTTPS) – minimamente – nas versões:

1.6.3.3.1. Microsoft Edge 129;

1.6.3.3.2. Safari 17;

1.6.3.3.3. Mozilla Firefox 125;

1.6.3.3.4. Google Chrome 129.

1.6.3.4. Deverá ter a possibilidade de exportar logs para servidores de Syslog e possibilitar a integração com dispositivos SIEM (*Security Information and Event Management*);

1.6.3.5. Deverá ter a possibilidade de enviar eventos via e-mail baseado em filtros e/ou critérios preestabelecidos;

1.6.3.6. Todos os eventos e ações realizadas na console deverão ser passíveis de monitoração para fins de auditoria;

1.6.3.7. Deverá ter painéis (*dashboards*) ou interfaces de gerência para facilitar a monitoração.

1.6.4. Deverá possuir funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados da solução ou fornecer ferramenta para tal finalidade;

1.6.5. Deverá permitir a configuração de senha para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço;

1.6.6. Deverá ter capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

1.6.7. Deverá ter a possibilidade de automatizar e programar as atualizações dos *softwares*;

1.6.8. A solução de gerência deve ter a capacidade de apurar e apresentar a

evolução de consumo das métricas básicas de dimensionamento das licenças/subscrições;

2. MÓDULO DE TRATAMENTO DE INCONSISTÊNCIAS

Durante o processo de deduplicação, é possível que sejam identificadas inconsistências nos dados biométricos ou biográficos de cidadãos. Essas inconsistências podem ser causadas por erros de coleta, alterações nas características físicas ao longo do tempo ou problemas com a integração dos dados. O módulo de tratamento de inconsistências será responsável por:

2.1. Gerenciar registros em conflito: Identificar e tratar os casos em que não há correspondência clara entre os dados biométricos e os registros existentes;

2.2. Resolver problemas de deduplicação: Garantir que as inconsistências sejam corrigidas de forma eficaz, assegurando que cada cidadão tenha um registro único e consistente;

2.3. O tratamento de exceções biométricas deve permitir a um operador analisar e resolver os casos em que o sistema encontra uma duplicidade em um novo cadastro ou em que não ocorre o casamento da biometria cadastrada com a nova em uma atualização, avaliando assim casos que podem sinalizar uma tentativa de fraude.

3. SEGURANÇA DA INFORMAÇÃO

3.1. Quanto ao fornecedor:

3.1.1. Possuir certificação em segurança da Informação válida (Ex. 27001/NIST);

3.1.2. Autorizar auditoria pela Dataprev em processos relacionados ao desenvolvimento de software e gestão de segurança da informação;

3.1.3. Realizar verificações de segurança junto a seus fornecedores;

3.1.4. Manter um processo de gestão do ciclo de vida do software;

3.1.5. Implementar processo robusto de gestão de incidentes de segurança da informação;

3.1.6. Apresentar à Dataprev comprovação dos requisitos de segurança sempre que solicitado.

3.2. Quanto à ferramenta:

3.2.1. Implementar Gestão de Controle de acesso granular baseado em papéis;

3.2.2. Implementar autenticação forte usando múltiplos fatores;

3.2.3. Implementar os princípios de Segurança e Privacidade por padrão e no desenho do produto;

3.2.4. Submeter-se a programa de gerenciamento de vulnerabilidades;

3.2.5. Implementar Registro de eventos (Logs) segmentado de maneira a identificar cada acesso a dado pessoal;

3.2.6. Permitir a integração dos registros de eventos a ferramentas de correlação de eventos;

3.2.7. Implementar Criptografia aos dados em trânsito;

3.2.8. Implementar Criptografia aos dados em repouso;

3.2.9. Prever mecanismo para exclusão de registros em conformidade com as legislações pertinentes;

3.2.10. Prever mecanismo de mascaramento de dados de acordo com os cenários de utilização, considerando a legislação vigente, conforme aplicável.

4. INFRAESTRUTURA ALOCADA

Os itens que não necessitarão de comprovação prática na prova de conceito estarão destacados neste anexo, com o termo “aceita-se documentação”.

4.1. Os componentes de software que integram o ambiente da solução serão instalados em máquinas virtuais oferecidas pela Dataprev e deverão ser compatíveis com os virtualizadores VMware, Microsoft Hyper-V, XenServer-Citrix; aceita-se documentação.

4.1.1. A fabricante deve comprovar suporte a API para NSX-T versão 3.2.X em vSphere conforme tabela de compatibilidade da VMWare. aceita-se documentação.

4.2. A solução deverá ter capacidade de gerar pacote de autodiagnostico de modo a coletar arquivos relevantes para envio ao suporte do produto;

4.3. O licenciamento, incluindo a gerência, deverá ter a atualização de software vigente até o término da garantia. Ao término da vigência da garantia dos softwares instalados não deverão perder a validade; aceita-se documentação.

4.4. A Dataprev fornecerá a infraestrutura virtualizada para o funcionamento da solução, limitando seus recursos – em cada site – da seguinte forma:

				Armazenamento

	Servidores Físicos de 2U	Núcleos de Processamento	Memória (TB)			
				Storage All-Flash (TB)	NFS (GB)	Banco de Dados (TB)
Ano 1	10	560	4	100	500	10
Ano 5	18	1.100	12	600	500	50

4.5. Os recursos não terão hardwares dedicados, ou seja, serão distribuídos nos clusters de tecnologia e de rede já criados e em funcionamento na Dataprev, obedecendo os limites equivalentes citados no item anterior;

4.6. Deverá efetuar log e gerar relatório;

4.7. A solução deverá possibilitar o funcionamento no mínimo nas seguintes tecnologias (caso sejam necessárias) ou versões superiores:

4.7.1. Sistemas Operacionais:

4.7.1.1. Linux Red Hat 9 ou

4.7.1.2. Windows Server 2022;

4.7.2. Virtualização:

4.7.2.1. VMware vSphere 6.7 e

4.7.2.2. VMware NSX-T versão 3.2;

4.7.3. Bancos de Dados:

4.7.3.1. Oracle DB 19c ou

4.7.3.2. SQL Server 2022;

4.7.4. Middleware:

4.7.4.1. Red Hat JBoss 7.4 ou

4.7.4.2. Oracle Weblogic 12.2.1.4 ou

4.7.4.3. SpringBoot 3.x

4.7.5. Balanceamento de Carga F5:

4.7.5.1. BigIP i5800 (global) e

4.7.5.2. BigIP i7800 (local)

4.7.6. Soluções de Códigos Maliciosos;

4.7.7. Proteção de dados DellEMC Power Protect, contendo:

4.7.7.1. Data Domain 9900 – DDOS 7.7.5.25;

4.7.7.2. ECS EX500 v3.8.0.3

4.7.7.3. Avamar 19.4

4.7.7.4. Networker 19.9.0.1

4.7.7.5. PPDM 19.15

4.8. Qualquer *software* diferente dos citados acima, se necessários para o funcionamento da solução, deverão ser fornecidos, licenciados, gerenciados e suportados pela proponente.

*** Este documento se torna válido a partir da assinatura de todos os signatários indicados em seu corpo, estando automaticamente invalidadas as assinaturas realizadas por usuários não indicados explicitamente no corpo deste documento.**

Documento assinado eletronicamente por **Saulo Milhomem dos Santos**, **Superintendente**, em 15/10/2024, às 23:45, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Lucio Antoniolo Netto**, **Gerente de Departamento**, em 16/10/2024, às 09:25, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Lauro Iatskiu Junior**, **Assessor(a) II**, em 16/10/2024, às 09:30, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Roberto Marinho Fernandes**, **Analista de TI**, em 16/10/2024, às 10:12, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Felipe de Sousa Freitas Pintos**, **Assessor(a) II**, em 16/10/2024, às 10:45, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fabricio Salles da Costa**, **Gerente de Divisão**, em 16/10/2024, às 11:10, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Helder Rocha Figueiredo**, **Superintendente. Substituto(a)**, em 16/10/2024, às 12:01, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Vinicius de Araujo Porto**, **Superintendente**, em 16/10/2024, às 13:54, conforme horário oficial de Brasília, com fundamento no Decreto nº 8.539, de 8 de outubro de 2015 e no Decreto n° 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://dataprev.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0072341** e o código CRC **8F5F3179**.

Referência: Processo nº 44129.011805/2024-93 SEI nº 0072341