ESTUDO TÉCNICO PRELIMINAR

PROCESSO ADMINISTRATIVO ELETRÔNICO Nº

Contratação de pessoa jurídica especializada em Tecnologia da Informação para prestação de serviços de atualização, desenvolvimento e customização de ecossistema de software legislativo; fornecimento, instalação e integração de infraestrutura de hardware para votação e presença com biometria facial; além de suporte técnico e manutenção preventiva e corretiva continuada, visando ao projeto, sustentação, operação assistida e evolução dos sistemas Legislativo, Administrativo e de Votação Eletrônica, incluindo o fornecimento de painéis de LED, terminais de autoatendimento, aplicação móvel (Super APP) e infraestrutura de servidores em nuvem para a Câmara Municipal do Recife.

ESTUDO TÉCNICO PRELIMINAR - ETP

1. INTRODUÇÃO

Estudo Técnico Preliminar (ETP) consiste no instrumento inicial da fase preparatória da licitação ou, se for o caso, da contratação direta, no qual se expõem o interesse público e a melhor solução sob os aspectos mercadológico, técnico, ambiental, cultural e econômico da contratação, com o objetivo de indicar a viabilidade da contratação e servir de base para edição do Termo de Referência ou Projeto Básico. O ETP indicará os problemas a serem resolvidos e concluirá pela melhor solução evidenciada, considerando a gestão, os riscos e os aspectos mercadológico, técnico, ambiental, cultural e econômico da contratação. Este instrumento terá o objetivo de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.
Referente ao Processo Administrativo eletrônico nº
Setor Requisitante: Divisão de Informática
Responsável pela Demanda: Ricardo Williams Paixão Ferraz
Área Técnica: Divisão de Informática
Data: 23 de março de 2026.
Fundamentação jurídica: art. 18, §§ 1º e 2º, da Lei Federal nº 14.133/2021.

2. DESCRIÇÃO DA NECESSIDADE

2.1. Necessidade de Contratação de pessoa jurídica especializada em Tecnologia da Informação para fornecimento de solução integrada de modernização legislativa para a prestação de serviços de atualização, desenvolvimento e customização de ecossistema de software legislativo; fornecimento, instalação e integração de infraestrutura de hardware para votação e presença com biometria facial; além de suporte técnico e manutenção preventiva e corretiva continuada, visando ao projeto, sustentação, operação assistida e evolução dos sistemas Legislativo, Administrativo e de Votação Eletrônica, incluindo o fornecimento de painéis de LED, terminais de autoatendimento, aplicação móvel (Super APP) e infraestrutura de servidores em nuvem para a Câmara Municipal do Recife.

A demanda engloba a total integração entre os módulos, o uso de assinatura digital ICP-Brasil e o suporte técnico contínuo para assegurar a operabilidade e a segurança dos trabalhos da Câmara Municipal.

Em observância às diretrizes do parecer jurídico, a presente contratação é composta por duas naturezas distintas de execução:

Necessidades Pontuais (Intercorrentes ou Eventuais): Compreendem as etapas de atualização tecnológica, desenvolvimento customizado, licenciamento e implantação de infraestrutura física (conforme detalhado nos itens 1 a 11 do descritivo quantitativo). Tratam-se de entregas de objeto certo e execução finita, fundamentais para estabelecer a nova base operacional dos sistemas legislativo e administrativo.

Necessidades Permanentes: Compreendem os serviços de manutenção (preventiva, corretiva e evolutiva), suporte técnico especializado e infraestrutura de servidores em nuvem (conforme itens 12 a 21). Dada a essencialidade dessas ferramentas para a continuidade dos trabalhos parlamentares e a segurança dos dados biométricos, tais serviços possuem natureza contínua, sendo indispensáveis para garantir a operabilidade ininterrupta, a integridade jurídica e a sustentabilidade tecnológica da Câmara Municipal.

2.2. A presente contratação justifica-se pela necessidade de prover à Casa Legislativa uma plataforma tecnológica unificada, segura, de alta disponibilidade e aderente às melhores práticas de governança pública, destinada à automação e modernização dos processos legislativos,

administrativos e de votação eletrônica. Trata-se de solução essencial para assegurar a continuidade institucional, a publicidade dos atos parlamentares e a eficiência operacional das atividades do Poder Legislativo.

2.3. Fundamentação Jurídica

A contratação está amparada pelos seguintes dispositivos e normativos:

Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos)

• Art. 11, IV, (*"incentivar a inovação e o desenvolvimento nacional sustentável."*)

– princípios da eficiência, inovação e economicidade;

Art. 169

§ 1º Na forma de regulamento, a implementação das práticas a que se refere o caput deste artigo será de responsabilidade da alta administração do órgão ou entidade e levará em consideração os custos e os benefícios decorrentes de sua implementação, optando-se pelas medidas que promovam relações íntegras e confiáveis, com segurança jurídica para todos os envolvidos, **e que produzam o resultado mais vantajoso para a Administração, com eficiência, eficácia e efetividade nas contratações públicas.**

Art. 18

§ 1º O estudo técnico preliminar a que se refere o inciso I do caput deste artigo deverá evidenciar o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação, e conterá os seguintes elementos:

IX - demonstrativo dos **resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis;**

• Padronização de soluções, compatibilidade tecnológica e uso de normas técnicas;

Art. 40

V - atendimento aos princípios:

a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;

• Art. 18 – planejamento da contratação e ETP;

I - a descrição da necessidade da contratação fundamentada em estudo técnico preliminar que caracterize o interesse público envolvido;

• Art. 42 ao 44 – segurança da informação, mitigação de riscos e requisitos mínimos tecnológicos;

Art. 42. A prova de qualidade de produto apresentado pelos proponentes como similar ao das marcas eventualmente indicadas no edital será admitida por qualquer um dos seguintes meios:

I - comprovação de que o produto está de acordo com as normas técnicas determinadas pelos órgãos oficiais competentes, pela Associação Brasileira de Normas Técnicas (ABNT) ou por outra entidade credenciada pelo Inmetro;

II - declaração de atendimento satisfatório emitida por outro órgão ou entidade de nível federativo equivalente ou superior que tenha adquirido o produto;

III - certificação, certificado, laudo laboratorial ou documento similar que possibilite a aferição da qualidade e da conformidade do produto ou do processo de fabricação, inclusive sob o aspecto ambiental, emitido por instituição oficial competente ou por entidade credenciada.

Art. 43. O processo de **padronização** deverá conter:

I - parecer técnico sobre o produto, considerados especificações técnicas e estéticas, desempenho, análise de contratações anteriores, custo e condições de manutenção e garantia;

II - despacho motivado da autoridade superior, com a adoção do padrão;

III - síntese da justificativa e descrição sucinta do padrão definido, divulgadas em sítio eletrônico oficial.

§ 1º É permitida a padronização com base em processo de outro órgão ou entidade de nível federativo igual ou superior ao do órgão adquirente, devendo o ato que decidir pela adesão a outra padronização ser devidamente motivado, com indicação da necessidade da Administração e dos riscos decorrentes dessa decisão, e divulgado em sítio eletrônico oficial.

§ 2º As contratações de soluções baseadas em software de uso disseminado serão disciplinadas em regulamento que defina processo de gestão estratégica das contratações desse tipo de solução.

Art. 44. Quando houver a possibilidade de compra ou de locação de bens, o estudo técnico preliminar deverá considerar os custos e os benefícios de cada opção, com indicação da alternativa mais vantajosa..

Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI)

A implantação de sistema legislativo integrado com ferramenta de streaming e painéis de votação cumpre o dever legal de publicidade dos atos parlamentares,

transparência ativa e disponibilização de informações em formato aberto.

1.3. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)

A solução contempla coleta, tratamento e armazenamento de dados biométricos (dados sensíveis), exigindo:

- Provedores certificados,
- Logs auditáveis,
- Criptografia forte,
- Governança de dados,
- Mecanismos de minimização, anonimização e gestão de consentimento.

1.4. Lei nº 14.129/2021 – Lei do Governo Digital

- A contratação promove:
- Transformação digital;
- Interoperabilidade;
- Redução de papel ("zero papel");
- Serviços digitais a usuários internos e externos.

2.4. Fundamentação Técnica:

A operação do Poder Legislativo moderno exige a disponibilização de infraestrutura tecnológica capaz de assegurar **celeridade, confiabilidade, segurança, imutabilidade, rastreabilidade e publicidade dos atos parlamentares**. A solução a ser contratada integra:

- Desenvolvimento de nova versão de sistema integrado de votação eletrônica, a partir de requisitos existentes e integração completa com sistema de processo legislativo, biometria facial e digital, com fornecimento de código-fonte e treinamento;
- Desenvolvimento de aplicativo PWA para votação remota;
- Desenvolvimento de aplicativo de votação com reconhecimento facial para os tablets existentes;
- Desenvolvimento de Software para o posto de votação existente;
- Fornecimento e desenvolvimento de terminal de presença com reconhecimento facial;
- Fornecimento e projeto de Painel de Led Pixel Pitch de 3.91 mm multifuncional;
- Fornecimento e desenvolvimento de postos de votação com reconhecimento facial para votação e presença;
- Desenvolvimento de um Super APP

- Instalação e ativação do Painel de Led e video Wall;
- Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado;
- Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte

técnico especializado, com assinatura digital ICP-Brasil (Processo Legislativo);

- Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado, com assinatura digital ICP-Brasil (Processo Administrativo);
- Manutenção do painel de Led do plenário principal;
- Horas de desenvolvimento por demanda;

3. Necessidade da Contratação

A presente contratação é necessária porque:

Os sistemas atualmente utilizados encontram-se defasados, fragmentados, sem interoperabilidade e com limitações para autenticação biométrica e votação remota segura. Há demandas crescentes por segurança da informação, especialmente em razão do uso de dados biométricos sensíveis.

A solução busca converter o atual cenário de sistemas fragmentados em um ecossistema de plena interoperabilidade, integrando os fluxos legislativos e administrativos. Esta abordagem visa sanar demandas tecnológicas como a implementação de assinaturas digitais e biometria facial, garantindo que a modernização atenda a requisitos de segurança e agilidade que não são suportados pelas plataformas utilizadas atualmente.

O Poder Legislativo depende de um ambiente integrado que impeça falhas, fraudes, duplicidade de votação e inconsistências documentais; A ausência de solução integrada compromete a continuidade administrativa, a publicidade das sessões e a qualidade da informação disponibilizada ao cidadão.

A presente contratação é imprescindível para garantir a atualização tecnológica e a segurança dos processos deliberativos e administrativos da Câmara Municipal. A justificativa se pauta nos seguintes pontos:

Modernização da Infraestrutura: A aquisição de um novo Painel de LED de alta definição (Pixel Pitch 3.91 mm) é essencial para substituir os atuais dispositivos de exibição. A nova tecnologia permitirá uma comunicação visual mais nítida, garantindo aos parlamentares e cidadãos a transparência imediata dos resultados das votações, presença e multimídia.

Continuidade e Evolução da Segurança Biométrica: A contratação visa dar continuidade ao padrão de segurança já estabelecido na Casa (votação com reconhecimento facial), fornecendo novos terminais e softwares atualizados que garantam maior agilidade no reconhecimento.

Expansão da Mobilidade: A necessidade de aprimorar a votação remota via aplicativo (PWA e Super APP) e tablets integrados à base de dados biométrica.

Sustentabilidade Tecnológica e Suporte: A necessidade de garantir manutenção evolutiva e corretiva assegura que a solução executada não se torne obsoleta em curto prazo, permitindo adaptações futuras.

4. Complexidade Técnica da Solução

Trata-se de solução tecnológica complexa, que exige:

Desenvolvimento de horas técnicas, distribuídas entre engenharia de software, UX/UI, segurança cibernética, criptografia, infraestrutura, testes, QA e homologação;

Uso de algoritmos de reconhecimento facial em conformidade com resoluções da ANPD;

Infraestrutura de alta disponibilidade (≥ 99,5%);

Painéis eletrônicos de alto desempenho, integrados ao motor de votação; Ambiente seguro com autenticação multifatorial e logs imutáveis.

A complexidade e o nível de integração descartam soluções genéricas de mercado, impondo a necessidade de empresa com domínio em tecnologia legislativa, votação eletrônica e biometria facial.

5. Riscos da Não Contratação

A não contratação acarretaria:

Descontinuidade das atividades plenárias;

Vulnerabilidade a fraudes, adulterações e falhas de registro;

Interrupção do controle de presença;

Falhas graves no processo deliberativo;

Descumprimento de obrigações legais de transparência;

Inobservância à LGPD na coleta e armazenamento de dados biométricos;
Perda de integridade da cadeia de custódia digital dos atos legislativos.

6. Benefícios e Resultados Esperados

Modernização completa do processo legislativo;

Redução de custos operacionais no médio e longo prazo;

Aumento da transparência e do controle social;

Maior segurança jurídica nas votações; Redução de fraudes e inconsistências;

Aderência a padrões internacionais de segurança (OWASP, ISO 27001);

Operações legislativas sem falhas, com redundância e auditoria completa.

Integração Total e Automatizada: Eliminação de lacunas operacionais entre o sistema de votação biométrica e o processo legislativo já existente. O resultado esperado é um fluxo de dados contínuo.

Modernização da Experiência Visual em Plenário: Substituição da infraestrutura de exibição antiga por painéis de LED de alta resolução, resultando em maior clareza na apresentação de matérias, transparência instantânea dos votos e capacidade de reprodução multimídia superior durante as sessões.

Otimização de Performance e Estabilidade: Atualização da arquitetura de software e banco de dados para garantir tempos de resposta mais ágeis no painel e no sistema de gestão, prevenindo lentidão e falhas decorrentes da obsolescência das versões atuais.

Eficiência na Gestão de Sessões: Redução do tempo operacional para abertura de votações, contagem de quórum e apresentação de resultados, devido à interface modernizada do painel e à integração em tempo real com a base de dados do processo legislativo.

Garantia de Ciclo de Vida Prolongado (Sustentabilidade): Manutenção da solução através de um regime de suporte e manutenção permanentes (corretiva e evolutiva). O resultado esperado é a eliminação do risco de obsolescência sistêmica, assegurando que o software e o hardware evoluam conforme as novas demandas da Câmara.

Resiliência e Continuidade Administrativa: Estabelecimento de um fluxo de suporte técnico especializado que garanta a operabilidade ininterrupta dos sistemas, minimizando o tempo de indisponibilidade e protegendo o investimento contra falhas críticas de infraestrutura.

Maximização da Segurança Consolidação de um ambiente de votação mais seguro por meio do reconhecimento facial e da biometria digital através da integração nativa com o padrão de assinaturas ICP-Brasil.

7. Conclusão

A contratação mostra-se imprescindível, legalmente fundamentada, tecnicamente necessária e estrategicamente adequada para garantir a continuidade dos trabalhos legislativos, a integridade dos atos do parlamento e a observância plena das normas de governança digital e segurança da informação aplicáveis ao setor público.

Assim, resta plenamente justificada a contratação integrada do Sistema Legislativo, Administrativo, de Votação Eletrônica, aplicativo com Reconhecimento Facial, Ferramenta de Streaming, Postos de Votação, Painel Eletrônico e Terminais de Autoatendimento.

8. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE

CONTRATAÇÕES ANUAL, SEMPRE QUE ELABORADO, DE MODO A INDICAR O SEU ALINHAMENTO COM O PLANEJAMENTO DA ADMINISTRAÇÃO

A Câmara Municipal do Recife ainda não elabora o Plano de Contratações Anual, dada a facultatividade trazida pela Lei no 14.133/21, em seu art. 12, VII, em que o legislador utilizou o verbo 'poderá', ao se referir à elaboração do PCA pelos entes públicos.

Mesmo assim, a demanda se encontra em alinhamento com as diretrizes de gestão da entidade, além de ter alinhamento com as peças orçamentárias, como será demonstrando da indicação da dotação orçamentária devida.

9. REQUISITOS DA CONTRATAÇÃO

Contratação de pessoa jurídica especializada em Tecnologia da Informação para prestação de serviço de desenvolvimento e sustentação de softwares, engenharia de sistemas, infraestrutura tecnológica e soluções integradas para Casas Legislativas, visando ao projeto, desenvolvimento, customização, implantação, operação assistida, manutenção evolutiva, corretiva e adaptativa, bem como ao suporte técnico contínuo de Sistema Legislativo, Administrativo e de Votação Eletrônica existentes da Câmara Municipal.

A empresa contratada deverá possuir os seguintes requisitos:

Ter experiência no objeto do contrato, que é a locação de software para a gestão de gabinetes incluindo a implantação, personalização de layout, treinamento, manutenção preventiva e corretiva com atualizações automáticas, hospedagem dos sistemas. Possuir o registro do software a ser locado no INPI (Instituto Nacional de Propriedade Industrial).

10. ESTIMATIVA DA QUANTIDADE DE BENS E/OU SERVIÇOS

Por tratar-se de serviço continuado, é estimada a quantidade de 60 meses para a vigência do contrato, de modo a garantir o funcionamento da solução.

Descrição dos Serviços			
Item	**Descrição**	**Quantidade**	**Unid.**
1	Atualização tecnológica de sistema integrado de votação eletrônica, a partir de requisitos existentes e integração completa com sistema de processo legislativo, biometria facial e digital, com fornecimento de código-fonte e treinamento	2500	horas
2	Atualização de aplicativo PWA para votação remota	120	horas
3	Atualização Aplicativo de votação com reconhecimento facial para o tablet	120	horas
4	Atualização de Software para o posto de votação existente	1000	horas
5	Desenvolvimento Postos de votação com reconhecimento facial para votação e presença (Móvel)	4	Equipamentos
6	Desenvolvimento Terminal de presença com reconhecimento facial	4	terminais
7	Desenvolvimento de Software para terminal de presença com reconhecimento Facial	900	horas
8	Metragem para painel LED Pixel Pitch de 3,91 mm (m2) com suporte e instalação inclusa)	25	metros
9	Atualização e ampliação Terminal de autoatendimento	15	unid.
10	Desinstalação do vídeo Wall existente no plenário atual e reinstalação nos demais ambientes da casa legislativa	1	desinstalação e reinstalação
11	Desenvolvimento Super APP	4500	horas

Manutenção mensal da solução			
Item	**Descrição**	**Quantidade**	**Unid.**
12	Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado(PAINEL ELETRÔNICO)	12	meses
13	Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado, com assinatura digital ICP-Brasil (Processo Legislativo)	12	meses
14	Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado, com assinatura digital ICP-Brasil (Processo Administrativo)	12	meses
15	Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do Software e hardware do posto de votação com biometria digital e facial	12	meses
16	Manutenção preventiva, corretiva, evolutiva,	12	meses

	atualizações de versão e suporte técnico especializado do software e Hardware do terminal de presença com reconhecimento facial		
17	Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do Super APP	12	meses
18	Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte do painel de Led.	12	meses
19	Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do terminal de autoatendimento	12	meses
20	Servidores em nuvem para aplicação	12	meses

Horas de desenvolvimento por demanda			
Item	**Descrição**	**Quantidade**	**Unid.**
21	Sistema de Painel Eletrônico	900	horas
22	Sistema de Processo Legislativo	800	horas
23	Sistema de Processo Administrativo	800	horas
24	Super App	1.200	horas
25	Posto de Votação coletivo	100	horas
26	Posto de Votação biometria facial e digital	100	horas
27	Sistema de Terminais de Autoatendimento	100	horas
28	Total de hora anual	4.000	horas
29	Total de hora cinco anos	20.000	horas

Quanto à modelagem de custos e execução dos serviços, os itens referentes ao desenvolvimento, customização e atualizações tecnológicas de softwares e infraestrutura possuem natureza de custo pontual, sendo pagos uma única vez após a efetiva entrega das

soluções. Em contrapartida, os serviços de manutenção preventiva, corretiva e evolutiva, bem como o suporte técnico especializado configuram-se como atividades permanentes e contínuas, visando garantir a sustentabilidade tecnológica, a segurança e a operabilidade ininterrupta dos sistemas da Câmara Municipal ao longo de toda a vigência contratual.

11. LEVANTAMENTO DE MERCADO E ANÁLISE DAS SOLUÇÕES

Não aplicável, por tratar-se de solução própria desta Casa Legislativa, devendo os serviços serem executados na plataforma existente.

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

A estimativa de custos está baseada para o período de 12(doze) meses.

O custo estimado para execução do projeto é de:

1 Prestação de Serviços de Atualização Tecnológica e novos desenvolvimentos R$ 4.991.700,00(Quatro milhões novecentos e noventa e um mil e setecentos reais)

2 Manutenção dos Serviço R$ 1.932.000,00 (Um Milhão novecentos e trinta e dois mil reais)

3 Banco de Horas de desenvolvimento por demanda/ano: 4.300, cujo Valor Total estimado anual é de : R$ 1.634.000 (Um milhão seiscentos e trinta e quatro reais)

Valor Total estimado: R$ 6.923.700,00 (seis milhõe, novecentos e vinte e três mil e setecentos reais)

- Atualização e Desenvolvimento
  - Atualização tecnológica de sistema integrado de votação eletrônica, a partir de requisitos existentes e integração completa com sistema de processo legislativo, biometria facial e digital, com fornecimento de código-fonte e treinamento - 2.500 horas
  - Atualização de aplicativo PWA para votação remota - 120 horas
  - Atualização Aplicativo de votação com reconhecimento facial para o tablet - 120 horas
  - Atualização de Software para o posto de votação existente - 1.000 horas
  - Desenvolvimento de Software para terminal de presença com reconhecimento Facial - 900 horas
  - Desenvolvimento Super APP - 4.500 horas

- Hardware

  - Desenvolvimento Postos de votação com reconhecimento facial para votação e presença (Móvel) - 4 postos
  - Desenvolvimento Terminal de presença com reconhecimento facial - 4 terminais
  - Metragem para painel LED Pixel Pitch de 3,91 mm (m2) com suporte e instalação inclusa) - 25 metros
  - Atualização e ampliação Terminal de autoatendimento - 15 unidades

- Manutenção
  - Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado(PAINEL ELETRÔNICO) - 12 meses
  - Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado, com assinatura digital ICP-Brasil (Processo Legislativo) - 12 meses
  - Manutenção (preventiva, corretiva e evolutiva), atualizações de versão e suporte técnico especializado, com assinatura digital ICP-Brasil (Processo Administrativo) - 12 meses
  - Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do Software e hardware do posto de votação com biometria digital e facial - 12 meses
  - Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do software e Hardware do terminal de presença com reconhecimento facial - 12 mesesManutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do Super APP - 12 meses
  - Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte do painel de Led. - 12 meses
  - Manutenção preventiva, corretiva, evolutiva, atualizações de versão e suporte técnico especializado do terminal de autoatendimento - 12 meses
  - Servidores em nuvem para aplicação - 12 meses
  - Desinstalação do vídeo Wall existente no plenário atual e reinstalação nos demais ambientes da casa legislativa - 1

- Banco de Horas de desenvolvimento por demanda/ano: 4.300 cujo valor total estimado para o item 3 é de : R$ 1.634.000 (Um milhão seiscentos e trinta e quatro reais)

13. JUSTIFICATIVA DO PARCELAMENTO OU NÃO DA LICITAÇÃO

A presente contratação não comporta parcelamento do objeto, tendo em vista a natureza integrada, contínua e interdependente dos serviços a serem prestados. As atividades de desenvolvimento e sustentação de softwares, engenharia de sistemas, infraestrutura tecnológica e fornecimento de soluções integradas para Casas Legislativas constituem um conjunto único e indivisível, cujo pleno funcionamento depende da atuação coordenada e harmônica de uma única contratada.

O parcelamento do objeto poderia comprometer a eficiência, a segurança, a compatibilidade e a continuidade dos sistemas legislativos, administrativos e de votação eletrônica existentes na Câmara Municipal, uma vez que tais sistemas compartilham bases de dados, regras de negócio, arquiteturas tecnológicas e fluxos operacionais comuns. A fragmentação da execução entre diferentes fornecedores aumentaria significativamente os riscos de falhas de integração, conflitos técnicos, sobreposição de responsabilidades e dificuldades na apuraçãode responsabilidades em caso de incidentes, além de potencializar vulnerabilidades de segurança da informação.

Ademais, a contratação integrada assegura maior eficiência administrativa, padronização tecnológica, redução de custos operacionais indiretos e maior celeridade na resolução de demandas evolutivas, corretivas e adaptativas, bem como na prestação do suporte técnico contínuo. Assim, o não parcelamento do objeto encontra amparo nos princípios da eficiência, economicidade, segurança e interesse público, estando plenamente justificado sob os aspectos técnico, operacional e gerencial, nos termos da legislação aplicável às contratações públicas.

14. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

1. Desenvolvimento de nova versão de sistema integrado de votação eletrônica, a partir de requisitos existentes e integração completa com sistema de processo legislativo, biometria facial e digital, com fornecimento de código-fonte e treinamento:

Consiste na contratação de empresa especializada em engenharia de software, com comprovada experiência em sistemas para o Poder Legislativo, para o desenvolvimento, evolução, integração, implantação, suporte e transferência de tecnologia de uma Nova Versão do Sistema Integrado de Votação Eletrônica, contemplando arquitetura moderna, segurança avançada, interoperabilidade e total aderência aos requisitos funcionais e técnicos já existentes no órgão.

1.1 Escopo Geral da Solução

O escopo compreende a análise, desenho, desenvolvimento, testes, homologação, implantação, capacitação e manutenção de um sistema integrado, modular e escalável, que engloba:

1.1.1 Módulo de Votação Eletrônica Presencial e Remota, com:

Registro criptografado de votos;

Auditoria em tempo real;

Múltiplos perfis de usuários (parlamentar, operador, presidente da sessão);

Suporte a votação nominal, simbólica, secreta, por destaque e por bloco.

1.1.2 Módulo de Reconhecimento Biométrico Misto, contendo:

Biometria facial com liveness detection (anti-spoofing);

Biometria digital integrada a dispositivos compatíveis;

Geração de logs invioláveis sobre presença e identidade do parlamentar;

Integração automática com o processo de identificação na abertura da sessão.

1.1.3 Integração Nativa e Bidirecional com o Sistema de Processo Legislativo (SPL) existente, contemplando:

Intercâmbio automático de vereadores em exercício, filiações partidárias, mesas diretora, proposições, pareceres, substitutivos e votações; Atualização em tempo real do status legislativo no SPL; Conformidade com modelos de dados pré-existentes; APIs RESTful e/ou SOAP baseadas em padrões abertos (OpenAPI, WSDL).

1.1.4 Disponibilização do Código-Fonte, incluindo:

Entrega integral do código fonte da solução e respectivos artefatos; Padrões de codificação, documentação e comentários técnicos;

Conformidade com o art. 6º, IX e art. 42 da Lei nº 14.133/2021, que amparam a transferência de tecnologia e garantem sustentabilidade da solução pelo órgão contratante.

Treinamento e Transferência de Conhecimento, abrangendo:

Capacitação técnica para equipe de TI;

Capacitação operacional para usuários internos;

Entrega de manuais técnicos, de operação e de manutenção;

Realização de workshops presenciais e/ou remotos.

1.2. Requisitos Técnicos e Arquiteturais

A solução deverá observar, no mínimo:

1.2.1 Arquitetura e Tecnologia

Arquitetura em microserviços ou multicamadas, de alta disponibilidade.

Suporte a containers (Docker, Kubernetes ou equivalente).

Front-end responsivo, compatível com dispositivos móveis.

Aplicação desenvolvida preferencialmente em Python 3.12, ou outra linguagem amplamente adotada e justificada tecnicamente.

Banco de dados relacional ou NoSQL escalável (PostgreSQL, MySQL, SQL Server, MongoDB etc.).

Protocolos seguros: TLS 1.3, HTTPS, OAuth2.0, OpenID Connect.

1.2.2 Segurança da Informação

Aderência à Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018).

Registro de logs imutáveis com carimbo do tempo.

Autenticação multifatorial para usuários administrativos. Criptografia dos dados em trânsito e em repouso.

Mecanismos automatizados de detecção de fraude biométrica.

1.2.3 Reconhecimento Biométrico

Precisão superior a 99% em FRR/FAR (padrões ISO/IEC 19795).

Algoritmos com certificações internacionais (NIST FRVT ou equivalentes).

Integração com câmeras Full HD e sensores biométricos de mercado.

1.3. Requisitos Jurídicos e Normativos

A contratação deverá observar:

Lei Nº 14.133/2021, especialmente:

Art. 6º – definição do objeto, requisitos técnicos e transferências de tecnologia;

Art. 20 – padronização e compatibilidade com sistemas existentes;

Art. 42 – requisitos para contratação de soluções de TI;

Art. 46 – inovação e desenvolvimento tecnológico;

Art. 74 – verificação de capacidade técnica;

Art. 75 – sustentabilidade e garantia de continuidade.

Instrução Normativa SGD/ME nº 94/2022 – Regras para contratações de TI no setor público:

Análise de riscos;

Sustentação tecnológica;

Entrega de código-fonte quando aplicável.

Decreto nº 10.046/2019 – Interoperabilidade entre plataformas governamentais.

Normas ISO/IEC:27001 (Segurança da Informação);

1.4. Ciclo de Desenvolvimento

A contratada deverá executar todas as etapas conforme metodologia Ágil (Scrum/Kanban) ou Cascata/Híbrida, conforme definido pelo órgão, incluindo:

Levantamento e refinamento dos requisitos existentes;

Elaboração do documento de arquitetura;

Modelagem de dados e APIs;

Prototipação; Desenvolvimento incremental;

Testes unitários, integrados, funcionais e de carga;

Homologação com o órgão;

Implantação em ambiente produtivo;

Treinamento e transferência de conhecimento.

Será exigido relatório de horas dedicadas, com rastreabilidade entre requisitos, tarefas, sprints e entregáveis.

Infraestrutura e Integrações

A solução deverá ser compatível com:

Estrutura de rede do órgão;

Servidores on-premise ou cloud (Azure, AWS, GCP ou equivalente);

Protocolos padronizados para integração;

Painéis de plenário, totens de presença, tablets, equipamentos biométricos e sistemas de áudio e vídeo.

2. Desenvolvimento de aplicativo PWA para votação remota:

Consiste na contratação de empresa especializada em desenvolvimento de software, com comprovada experiência em soluções legislativas, sistemas de

votação eletrônica e tecnologias de autenticação segura, para a concepção, desenvolvimento, testes, implantação, capacitação, suporte e transferência de tecnologia de um Aplicativo Web Progressivo (PWA) destinado à votação remota segura por parlamentares, plenamente integrado ao sistema legislativo e às ferramentas de gestão de sessões do órgão contratante.

Trata-se de solução inovadora, multiplataforma e compatível com navegadores modernos, permitindo participação remota em votações oficiais com elevados padrões de segurança, auditabilidade e conformidade legal.

2.1. Escopo Geral do PWA de Votação Remota

O desenvolvimento compreende a entrega de uma solução completa, que inclui:

2.1.1 Aplicativo PWA responsivo e instalável

Funcionamento em navegadores modernos (Chrome, Edge, Firefox, Safari); Modo instalável em smartphones, tablets e desktops, com ícone próprio; Operação mesmo em condições de baixa conectividade (offline-first, quando aplicável);
Sincronização automática de dados quando a conexão é restabelecida;

Suporte a push notifications e atualização automática de versões.

2.1.2 Funcionalidades de votação remota avançadas

2.1.3 Participação remota em votações plenárias e de comissões;

Registro criptografado da manifestação do voto e confirmação digital;

Exibição de pauta, proposições, substitutivos, orientações de bancada e resultados em tempo real;

Fluxo de abertura de sessão, chamada, verificação de quórum e controle de presença;

Suporte a voto secreto e voto aberto, conforme o regimento interno do órgão.

2.1.4 Autenticação forte e validada

Autenticação de múltiplos fatores (MFA);

Revalidação de identidade durante a sessão quando necessário; Registro de logs invioláveis para garantir autoria e integridade.

2.1.5 Reconhecimento biométrico facial e/ou digital integrado

Confirmação de identidade no momento da votação;

Algoritmos com detecção de vida (liveness detection) para evitar fraude;

Aderência a padrões internacionais de biometria (ISO/IEC 30107).

2.1.6 Integração completa com o Sistema de Processo Legislativo (SPL)

Envio automático dos votos para registro oficial;

Atualização de quórum e presença;

Sincronização de proposições, matérias legislativas, orientações e relatórios;

APIs RESTful seguras e documentadas.

2. Requisitos Técnicos da Solução

2.2.1 Tecnologias e Arquitetura

Desenvolvimento em frameworks modernos para PWA (Next.js ou equivalente);
Backend robusto, escalável e seguro (linguagem Python);
Banco de dados com replicação e alta disponibilidade (PostgreSQL, MySQL, SQL Server etc.);

Comunicação via APIs REST/RESTful com JWT, OAuth 2.0 ou OpenID Connect;

Suporte a Service Workers para operação PWA completa.

Segurança e Criptografia

A solução deve atender aos mais elevados padrões de segurança digital:

Criptografia ponta a ponta (E2EE) e criptografia em repouso;

Assinatura digital dos votos e logs de auditoria com carimbo de tempo;

Proteção contra ataque de repetição (replay attack), hijacking, phishing e MITM;

Uso de TLS 1.3 ou superior;

Controle de acesso baseado em perfis e políticas (RBAC ou ABAC).

2.2.2 Conformidade com a LGPD

Deverá observar integralmente a Lei Geral de Proteção de Dados (Lei nº 13.709/2018):

Coleta mínima necessária;

Consentimento, quando aplicável; Mapa de dados e análise de riscos;

Controlador e Operador definidos no contrato;

Tratamento adequado de dados biométricos, considerados sensíveis.

2.3. Requisitos Jurídicos e Normativos Aplicáveis

A contratação deve observar rigorosamente os marcos legais pertinentes:

2.3.1 Lei nº 14.133/2021 – Nova Lei de Licitações

Art. 6º, XX — definição de soluções de tecnologia da informação;

Art. 20 — necessidade de padronização e interoperabilidade;

Art. 42 — requisitos específicos para contratações de TI;

Art. 46 — contratações de inovação tecnológica;

Art. 74 — comprovação de capacidade técnica.

2.3.2 Regimento Interno do Poder Legislativo

Observância das regras de votação (aberta/secreta), quórum, presença e ordem das sessões;

A tecnologia deverá suportar os cenários regimentais.

2.3.3 Normas e padrões internacionais

2.3.4 ISO 27001 – Segurança da Informação;

2.4. Ciclo de Desenvolvimento e Entregáveis

2.4.1 Metodologia

A contratada deverá utilizar metodologia Ágil (Scrum/Kanban) ou híbrida, devendo entregar:

Sprints quinzenais ou mensais;

Backlog de requisitos priorizados;

Demonstrações periódicas;

Registro de horas dedicadas a cada atividade.

2.4.2 Entregáveis mínimos

Levantamento de requisitos e documentação funcional; Documento de arquitetura da solução (DAS); Protótipos e wireframes navegáveis;

Aplicativo PWA completo;

Backend e APIs documentadas com OpenAPI/Swagger; Scripts de implantação e manuais técnicos; Documentação de segurança e análise de riscos; Código-fonte completo em repositório Git;

Testes (unitários, integrados, segurança, carga e homologação);

Plano de Capacitação e Treinamento;

Suporte técnico durante todo o período contratual.

2.5. Integração e Infraestrutura

O PWA deverá ser compatível com:

Infraestrutura do órgão (on-premise, cloud ou híbrida); Servidores web de alta disponibilidade;
CDN para otimização do acesso remoto;

Plataformas móveis iOS e Android (via navegador);

Servidores de streaming e painéis de plenário, quando aplicável.
Suporte, Manutenção e Sustentação

A contratada deverá prever:

Manutenção corretiva, evolutiva e adaptativa;

Atualização contínua de segurança;

Monitoramento de performance e logs;

SLA de atendimento e solução;

Garantia contra falhas de operação e vulnerabilidades.

3. Aplicativo de votação com reconhecimento facial para o tablet existente:

A presente descrição técnica tem por objetivo detalhar, para fins de Termo de Referência / Projeto Básico / Especificação Técnica, a solução de aplicativo de votação presencial a ser implantado em tablets já existentes no órgão contratante, com autenticação por reconhecimento facial e todos os mecanismos necessários para segurança, auditabilidade, integridade jurídica e conformidade com normas e legislação aplicáveis.

3.1. Objetivo da Solução

Desenvolver, fornecer, configurar e colocar em operação um aplicativo nativo/PWA otimizado para tablets existentes que permita:

autenticação segura de usuários (parlamentares/eleitores/mesários) por reconhecimento facial com liveness detection;

registro seguro e imutável de votos (nomeados e/ou anônimos conforme regimento);

integração com o Sistema de Processo Legislativo (SPL) e com sistemas de presença/quórum;

geração de trilhas de auditoria completas e relatórios de conformidade;

operação com alta usabilidade, performance e disponibilidade durante sessões.

3.2. Premissas e Compatibilidade com Tablet Existente

O aplicativo deverá suportar os tablets atualmente em uso pelo órgão. Caso haja variação de Sistema Operacional entre os aparelhos, a solução deverá contemplar:

Android (preferencial): app nativo (Kotlin/Java) ou PWA otimizado; uso de APIs nativas de câmera e sensores.

iOS: app nativo (Swift) ou PWA com adaptações específicas.

Windows (caso haja): app UWP/Win32 ou PWA compatível.

O fornecedor deve realizar inventário e teste de compatibilidade com os modelos entregues pelo contratante antes da homologação.

Requisitos mínimos sugeridos para o tablet (se necessário prever substituição): CPU multinúcleo modernas, RAM ≥ 3 GB, câmera frontal Full HD com suporte a 30+ FPS, armazenamento mínimo 32 GB, conexão Wi-Fi e, opcional, 4G/5G.
O app deve ser capaz de funcionar em condições de conectividade limitada (modo degradado) e sincronizar resultados quando a conexão for restabelecida, mantendo integridade e ordenação temporal dos eventos.

3.3. Arquitetura da Solução

Camada Cliente
(App no tablet) Interface
responsiva e acessível.
Módulo de captura facial (câmera frontal) com pré-processamento local (detecção de rosto, direcionamento de iluminação).
Módulo de liveness detection (anti-spoofing) executado preferencialmente no dispositivo;
fallback para verificação por servidor se hardware for limitado.
Módulo de criptografia local para assinatura e proteção temporária dos registros.
Cache seguro de eventos (logs e votos) para operação offline.
Camada Servidor / Backend
Serviços de autenticação, orquestração de sessões, registro definitivo de votos e logs.
Repositório seguro de dados e logs (banco relacional + armazenamento seguro para arquivos/mídia).
API RESTful (OpenAPI/Swagger) com autenticação via OAuth2 / OpenID Connect e tokens JWT.
Serviços de auditoria e geração de relatórios.
Integração
Conectores/API para o SPL, para sistemas de presença/quórum e para diretórios de usuários (LDAP/Active Directory).
Mecanismo de sincronização com garantia de idempotência e ordenação temporal.
Repositório de Biometrias
Se houver armazenamento de templates biométricos: repositório cifrado, segregação de funções, logs de acesso e políticas de retenção conforme LGPD.
Alternativa: validar comparações por template comparador remoto sem persistir templates no tablet.

3.4. Funcionalidades Principais

Autenticação inicial

Login por credencial primária (senha/certificado) + reconhecimento facial como fator de confirmação.

Opção de MFA (aplicação de token, OTP, smartcard ou certificado digital do usuário) para perfis administrativos.

Verificação de identidade (face)

Captura facial e verificação 1:1 contra template cadastrado.

Liveness detection para rejeitar spoofing (vídeo/mascara/foto).

Registro de probabilidade/score da verificação no log.

Fluxo de sessão e presença
Chamadas, controle de presença e atualização de quórum automático. Associação automática entre identidade validada e assento/parlamentar. Votação
Tipos suportados: nominal, simbólica, secreta (quando aplicável), por bloco, por destaque.

Confirmação do voto ao eleitor; possibilidade de cancelamento dentro de janela de timeout.

Geração de comprovante (hash assinado) visível ao usuário e registrável no backend.

Auditabilidade

Logs imutáveis (append-only) com carimbo temporal (timestamp) e assinatura digital.

Registro de eventos de captura facial, resultados de PAD, tentativas de fraude, desconexões,

sincronizações.

Administração e monitoramento

Painel de operações para monitorar status dos tablets, nível de bateria, conectividade e integridade dos dados.

Ferramentas de diagnóstico remoto e deploy.

3.5. Segurança e Proteção de Dados

Criptografia

Tráfego via TLS 1.3+.

Dados em repouso cifrados (AES-256 ou equivalente).

Assinaturas digitais dos registros (ex.: X.509) para garantir não-repúdio.

Proteção de Biometria (dados sensíveis)

Biometria tratada como dado sensível (LGPD): só coletar o mínimo necessário.

Preferência por armazenamento de templates em forma cifrada e com possibilidade de tokenização.

Política estrita de acesso, logs e anonimização quando exigido. Liveness / PAD

Implementação de técnicas combinadas: análise de textura, movimento, profundidade (se hardware suportar), análise por desafio (sorriso, virar cabeça, abrir olhos).

Registro do resultado do PAD e ações aplicadas (bloqueio, re-tentativa, verificação manual).

Hardening

Verificação do ambiente de execução (root/jailbreak detection).

Proteção contra replay e man-in-the-middle (nonces, timestamps, assinaturas).

Segurança de ciclo de vida

Processo formal de gestão de vulnerabilidades (CVE), atualizações seguras (OTA), e resposta a incidentes.

3.6. Conformidade Legal e Normativa

LGPD (Lei 13.709/2018):

Definir base legal para tratamento de dados biométricos (consentimento expresso, obrigação legal ou interesse público conforme aplicável).

Realizar Análise de Impacto à Proteção de Dados (DPIA/Relatório de Impacto).

Estabelecer papel de controlador/operador no contrato.

Plano de retenção e eliminação segura dos dados.

Requisitos regimentais:

Conformidade com regras de votação do regimento interno (voto secreto/aberto, prazos e quóruns).

Padrões internacionais recomendados:

ISO/IEC 30107 (Presentation Attack Detection), ISO/IEC 19795 (avaliação de desempenho biométrico), ISO 27001 (SGSI), ISO 25010 (qualidade de software).

3.7. Privacidade e Governança de Dados

Minimização de dados: armazenar apenas o necessário para comprovação da identidade e auditabilidade.

Transparência: geração de relatórios e registros de tratamento de dados acessíveis ao controlador.

Direito dos titulares: procedimentos para acesso, retificação, eliminação e portabilidade.

Contrato com cláusulas específicas sobre responsabilidades, segurança, vazamento e comunicações de incidentes em conformidade

com LGPD.

3.8. Testes, Homologação e Critérios de Aceitação

Testes obrigatórios:

Testes unitários e de integração (cobertura mínima a ser acordada).

Testes de segurança (pentest, análise de código estático e dinâmico).

Testes de performance e carga (simular sessão com X tablets concorrentes).

Testes de usabilidade (workflow de voto em ≤ N segundos).

Testes biométricos:

Taxas de FAR (False Accept Rate) e FRR (False Reject Rate) medidas em ambiente controlado.

Testes de PAD contra ataques plausíveis (foto, vídeo, máscara).

Testes de interoperabilidade com SPL e mecanismos de sincronização.

Critérios de aceitação (exemplos):

Autenticar 99% dos usuários legítimos em condições normais (metas ajustáveis).

FAR ≤ estabelecido em edital (ex.: 0,01% — a definir).

Capacidade de operação com até N tablets simultâneos sem perda de integridade.

Logs auditáveis e assinados para 100% das ações críticas.

3.9. Entregáveis

Aplicativo embalado para os modelos de tablet aprovados (APK/IPA/manifest para PWA).

Documentação de segurança e relatório de pentest.

Plano de migração e procedimento de instalação em massa.

Plano de testes e relatórios de homologação.

Procedimentos operacionais e manuais de usuário e administrador.

Plano de contingência e continuidade (procedimentos em caso de falha massiva).

Treinamento presencial/remoto para operadores e equipe técnica.

SLA e plano de manutenção / atualização.

3.10. Suporte, Manutenção e SLA

Suporte 1º/2º/3º nível com tempos de resposta e resolução definidos (ex.: resposta inicial em 2 h para incidente crítico).

Correções de segurança emergenciais com prazo contratual (ex.: 72 h para CVE crítico).

Atualizações regulares e releases de correção e melhoria.

Monitoramento remoto opcional e relatório mensal de saúde do sistema.

3.11. Gestão de Risco

Inventário e teste prévio dos tablets para identificar insuficiências de hardware.

Plano de fallback: votação manual com registro digitalizado em caso de indisponibilidade parcial.

Estratégias de mitigação para spoofing biométrico, perda de conectividade e ataques DDoS.

Seguro e cláusulas contratuais para cobertura de incidentes de segurança, quando aplicável.

3.12. Aspectos Contratuais Recomendados

Cláusulas de propriedade intelectual e transferência de tecnologia (entrega de código-fonte;

licenças de uso perpétuas para a administração pública).

Obrigações de segurança e confidencialidade estritas.

Cláusulas de penalidades por descumprimento de SLA e requisitos de desempenho.

Previsão de auditorias periódicas independentes e direito de inspeção técnica.

Garantia mínima e condições para suporte evolutivo pós-garantia.

3.13. Observações Operacionais e Boas Práticas

Preferir processamento biométrico on-device quando seguro e viável, para reduzir exposição de dados sensíveis.

Registrar hashes públicos dos resultados de votação em banco de dados imutável e assinado para fins de verificação externa (prova computacional de integridade).

Adotar logs separados por níveis e manter backups cifrados com políticas de retenção claras.

Realizar campanha de treinamento e simulados antes das primeiras votações oficiais.

4. Desenvolvimento de Software para o posto de votação existente:

4.1. Consiste na contratação de empresa com comprovada expertise em engenharia de software aplicada a sistemas de votação eletrônica, para o desenvolvimento de uma solução completa, robusta e de alta confiabilidade destinada ao posto de votação existente, compreendendo a criação de uma

plataforma moderna, integrada, segura e capaz de operar de forma harmônica com todas as demais soluções do ecossistema legislativo. O software deverá ser projetado para funcionar em sinergia com o hardware previamente instalado, maximizando sua capacidade operacional, estendendo a vida útil dos componentes e garantindo compatibilidade com requisitos tecnológicos contemporâneos, incluindo processamento de dados biométricos, comunicação segura com servidores centrais e execução de mecanismos de auditoria digital avançada.

4.2. Escopo Geral do Software

O desenvolvimento deverá contemplar o ciclo completo de engenharia de software e incluir:

4.2.1 Aplicativo dedicado ao Posto de Votação Interface otimizada para o hardware já existente (PC, terminal embarcado, mini-PC, thin-client ou equipamento proprietário).

Compatibilidade com telas touch, teclados físicos, leitores biométricos e dispositivos auxiliares instalados.

Lógica de votação segura, com alta confiabilidade e baixa latência.

Operação contínua durante sessões extensas, sem necessidade de reinicialização.

4.2.2 Integração com os periféricos e módulos existentes

O software deverá integrar-se, conforme disponível no equipamento:

Sensores biométricos (digital/facial).

Leitores RFID/NFC.

Botões físicos de voto, teclados direcionais e painéis físicos.

Displays secundários.

Controladores de acesso do posto (módulos USB, serial, GPIO).

Mecanismos de redundância e failover, quando disponíveis.

4.3. Arquitetura de Software

4.3.1 Componentização

A solução deverá ser estruturada em módulos independentes, incluindo:

Módulo de Interface Operacional do Eleitor/Parlamentar

Módulo de Autenticação e Identificação Biográfica/Biométrica

Módulo Criptográfico e de Assinatura Digital

Módulo de Comunicação (Message Broker/API Client)

Módulo de Logs e Auditoria

Módulo de Monitoramento e Telemetria

Módulo de Failover Operacional (fila local + reenvio seguro

4.3.2 Comunicação

A arquitetura deverá adotar:

Comunicação via API REST/RESTful ou WebSocket com criptografia fim a fim.

Protocolos mínimos: TLS 1.3, HSTS, Perfect Forward Secrecy.

Mecanismo de fila local persistente (Message Queue) para tolerância a falhas de rede.

4.3.3 Operação Offline e Re-Sincronização

Capacidade de operar mesmo em períodos curtos sem acesso ao servidor central.

Armazenamento local temporário cifrado.

Mecanismo de reenvio idempotente para evitar duplicidade de votos e eventos.

4.4. Requisitos Funcionais Avançados

4.4.1 Identificação do Usuário

O software deverá suportar um ou mais métodos:

Autenticação por login/senha ou cartão corporativo.

Identificação biométrica (digital ou facial), com verificação 1:1.

Integração com diretórios internos (LDAP/AD).

4.4.2 Fluxo de Sessão

Abertura e fechamento de sessões conforme sinal enviado pelo sistema de gestão legislativa.

Recebimento de pauta, proposições, substitutivos e orientações.

Controle de presença e registro de chamadas.

4.4.3 Fluxo de Votação

Votação de matérias únicas, múltiplas, destaques, blocos, votações urgentes e simbólicas.

Tipos de voto: Sim, Não, Abstenção, Obstrução, conforme regimento.

Suporte a voto secreto — anonimização obrigatória.

Registro criptográfico do voto com hash único.

4.4.4 Feedback ao Usuário

Interface responsiva com confirmações visuais e sonoras.

Indicação de resultado local e sincronização com o painel do plenário.

4.5. Requisitos de Segurança

4.5.1 Criptografia e Integridade

Assinatura digital de todos os votos e eventos.

Armazenamento em repouso utilizando AES-256 ou superior.

Hardening do SO onde o posto estiver instalado (política de restrição).

4.5.2 Auditoria e Logs

Logs assinados digitalmente e invioláveis (append-only).

Registro de:

Votos (anonimizados quando necessário)

Horário de cada ação

Falhas de autenticação

Erros e reenvios

Eventos críticos de rede e segurança

Carimbo temporal confiável (NTP

seguro).

4.5.3 Proteção Contra Ameaças

Detecção de tentativas de engenharia reversa.

Atualizações assinadas digitalmente.

Prevenção contra Replay Attack com tokens únicos por sessão.

Mecanismo de watchdog para reinicialização automática em

travamentos.

4.6. Compatibilidade com Infraestrutura Existente

4.6.1 Hardware, Software , Protocolos e APIs

A integração com o sistema principal deverá ocorrer via:

API REST, WebSocket, ou Message Broker (MQTT/RabbitMQ/ZeroMQ).

Documentação via OpenAPI/Swagger.

4.7. Padrões de Engenharia, Qualidade e Testes

4.7.1 Padrões

ISO/IEC 27001 – Segurança da Informação

4.7.2 Testes Obrigatórios

Testes unitários (cobertura mínima definida contratualmente).

Testes integrados com SPL e demais sistemas.

Testes de carga simultânea (múltiplos postos).

Testes de estresse do hardware.

Testes de segurança (Pentest interno/externo).

Testes de failover e persistência local.

Testes de UI/UX com grupos de usuários.

4.7.3 Homologação

Roteiro detalhado com cenários de:

quorum,

reconexã

o,

exceções de sessão,

votações múltiplas simultâneas.

4.8. Manutenção, Monitoramento e Atualizações

4.8.1 Monitoramento Contínuo

Telemetria do posto: CPU, RAM, rede, energia, disponibilidade.

Sistema central com dashboard para acompanhamento.

4.8.2 Atualizações OTA (Over the Air)

As atualizações do software devem ocorrer automaticamente e com:

pacote assinado;

verificação de integridade;

rollback seguro.

4.8.3 Suporte e SLA

Suporte com níveis estabelecidos (N1/N2/N3).

SLA de resolução técnica (ex.: incidentes críticos em 2 horas).

Monitoramento com alertas automáticos.

4.9. Documentação Técnica e Entregáveis

A contratada deverá fornecer:

Documento de arquitetura (DAS).

Documento de requisitos (FR e NFR).

Especificação de APIs e integrações (Swagger).

Diagramas UML (casos de uso, componentes, sequência). Código-fonte completo e repositório Git.

Manual operacional e manual de administrador.

Plano de testes e relatório final de homologação.

Plano de manutenção e suporte.

Plano de contingência para falhas em postos.

4.10. Conformidade Legal

O software deverá obedecer a todos os requisitos:

4.10.1 LGPD – Lei 13.709/2018

Política de privacidade.

Registro de operações.

Mecanismo de proteção a dados sensíveis.

Relatório de Impacto (quando necessário).

4.10.2 Lei 14.133/2021

Comprovação de capacidade técnica.

Conformidade com requisitos de segurança.

4.10.3 Regras regimentais

Tipos de votação e fluxos operacionais devem ser completamente aderentes ao regimento interno do órgão.

5. Terminal de presença com reconhecimento facial:

Consiste no desenvolvimento, fornecimento, integração e implantação de um Terminal de Presença Inteligente, dotado de tecnologias embarcadas de reconhecimento facial de alta precisão, integração com sistemas de controle de acesso e votação legislativa, mecanismos de segurança avançada, captura de dados biométricos, registro de presença com integridade legal e interoperabilidade plena com plataformas corporativas. A solução deverá operar de forma totalmente autônoma ou integrada a infraestrutura de TI existente, funcionando como um dispositivo confiável para o registro formal de

presença de parlamentares, servidores ou usuários autorizados, garantindo autenticidade, segurança e rastreabilidade do processo.

5.1. Finalidade da Solução

A solução tem como objetivo fornecer um terminal de presença moderno, capaz de realizar a identificação inequívoca de indivíduos por meio de reconhecimento facial, assegurando controle rigoroso de participação, presença e autenticação, especialmente em ambientes de alta sensibilidade institucional, como casas legislativas, tribunais, órgãos públicos e espaços corporativos. A solução deve permitir que o registro de presença seja executado com eficiência, rapidez e precisão, com mecanismos robustos de prevenção contra fraude, garantindo aderência às normativas de segurança da informação e à legislação vigente, inclusive no tratamento de dados biométricos.

5.2. Configurações Tecnológicas da Solução

5.2.1 Arquitetura de Hardware do Terminal

O Terminal de Presença deverá ser composto por hardware industrial de alta durabilidade, projetado para operação contínua (24x7), composto minimamente por:

VALIDADOR RECONHECIMENTO FACIAL:

Tela: 7 polegadas, 1280x800 pixels, com tela de

toque; Alto-falante para informações ao usuário;

Câmera 1.3 MP RGB + Câmera 1.3 MP IR;
Live detection (não permite uso de foto ou vídeo em meio físico ou digital); Capacidade armazenamento: 10.000 usuários;
Interface: Ethernet TCP/IP;

Tempo de verificação e liberação de acesso: menor que 1 segundo;

Distância de detecção: ajustável, via software, de 0,5 metros a 4 metros;

Precisão > 99,9% (1:N);

Baixo índice de falsa rejeição (FAR 0,01);

Medição de temperatura por infravermelho com precisão de 0,5 graus Celsius;

Suporte para fixação em parede com articulação horizontal e vertical;

INTEGRAÇÃO COM SISTEMA DE VOTAÇÃO

Através de software já desenvolvido para a solução de Tablets da Casa Legislativa que se conecta ao banco de dados do sistema de votação;

Envio da imagem e ID único do parlamentar para o controle de acesso;

Gravação da presença do parlamentar assim que o reconhecimento facial for

realizado;

5.3. Tecnologias de Reconhecimento Facial

5.3.1 Algoritmos e Modelos Biométricos

A solução deverá utilizar tecnologias de visão computacional baseadas em redes neurais profundas (Deep Neural Networks), preferencialmente modelos:

CNNs de última geração (ResNet, MobileFaceNet, EfficientNet ou ArcFace);

Modelos com performance validada em benchmarks internacionais, como NIST FRVT 1:1 e 1:N;

Capacidade de inferência local otimizada via frameworks como TensorFlow Lite, PyTorch

Mobile ou ONNX Runtime.

5.3.2 Precisão e

Desempenho O terminal

deve apresentar:

FRR (False Rejection Rate) inferior a 1%;
Capacidade de identificação 1:N de até 10.000 usuários cadastrados localmente; Tempo médio de autenticação < 1 segundo da detecção ao resultado.
5.3.3 Liveness Detection e Anti-Fraude

O dispositivo deve obrigatoriamente possuir:

Detecção de profundidade via IR;

Análise de textura, detecção de piscada e microexpressões;

Reconhecimento anti-spoofing para:

fotos

impressas, telas

digitais,

máscaras 3D,

vídeos reproduzidos.

5.4. Segurança da Informação e Proteção de Dados

5.4.1 Criptografia e

Proteções A solução deverá

implementar:

Criptografia nativa AES-256 para armazenamento local;

TLS 1.3 para comunicação com servidor;

Certificados digitais próprios ou assinados;

Hash de integridade (SHA-256 ou SHA-3) para logs;

Secure Boot e verificação criptográfica do firmware.

5.4.2 Compliance

Jurídico A solução

deve atender:

LGPD – especialmente no tratamento de dados biométricos sensíveis; Lei nº 14.133/2021 – contratação de TI com especificação detalhada; IN SGD/ME nº 94/2022 – diretrizes para contratações públicas de TI;

Normas ISO/IEC 27001 e ISO 27701 – gestão de segurança e privacidade.

5.5. Funcionalidades do Software Embarcado

O firmware/software do terminal deverá incluir:

5.5.1 Módulo de Captura e Processamento

Facial Enquadramento automático;

Filtros contra ruído e compensação de baixa luminosidade;

Detecção de rosto em milissegundos;

Extração local de características biométricas (face embedding).

5.5.2 Módulo de Autenticação

Suporte a autenticação 1:1 (verificação) e 1:N (identificação);

Capacidade de operar online e offline, com posterior sincronização segura;

Registro de impressões, tentativas, erros e eventos de segurança.

5.5.3 Módulo de Integração

Comunicação direta com APIs do sistema legislativo;

Envio automático de logs, registros de presença e eventos de autenticação;

Compatibilidade com padrões REST, JSON, MQTT e WebSocket.

5.5.4 Módulo de Gerenciamento e

Monitoramento Atualização remota de

firmware (OTA); Dashboard centralizado para

acompanhar:

status dos terminais,

estatísticas de autenticação,

falhas e alertas,

histórico de usuários.

5.6. Registro de Presença e Validade Jurídica

O terminal deverá registrar:

Data e hora sincronizadas via NTP certificado;

Hash criptográfico do evento;

ID biométrico e ID do usuário;

Resultado da identificação e condições ambientais;

UID da sessão de votação ou plenário (quando aplicável).

Os dados devem ser auditáveis e imutáveis, garantindo a rastreabilidade exigida em processos oficiais.

5.7. Requisitos Ambientais e Operacionais Temperatura operacional: 0°C a 50°C; Umidade: 10% a 90% sem condensação;

Ciclo de operação contínua: 24x7;

MTBF mínimo: 50.000 horas.

5.8. Entregáveis e Integração A contratada deverá fornecer:

Terminais configurados e testados;

Aplicativo embarcado completo com código-fonte;

APIs documentadas (Swagger/OpenAPI);

Manual de manutenção, instalação e operação;

Certificados de conformidade técnica;

Suporte e garantia pelo período definido no contrato;

Treinamento técnico para equipe operacional.

5.9. Possíveis Extensões da Solução (opcionais conforme edital)

Leitor biométrico digital integrado;

RFID ou cartão inteligente;

Impressão de comprovantes;

Integração com catracas/portas;

Módulos adicionais de confirmação sonora ou tátil.

5.10 Características do Módulo Facial

Gabinete:

– Acesso frontal para manutenção;

– Dotado de fechadura com chave com segredo;

– Ajuste de ângulo de inclinação

da tela; Parte Traseira:

– Fabricado em chapas de aço inox AISI304 de 1,0 mm de espessura;
– Aberturas de ventilação por convecção;

– Abertura para passagem dos cabos de rede

e energia; Parte Frontal:

– Injetado em plástico

ABS preto; Pedestal ou suporte

de parede:

– Fabricado em chapas de aço de 1,0 mm de espessura;

– Abertura para passagem dos cabos de rede e energia;

– Mecanismo de ajuste de inclinação do gabinete:

– Eixo de rotação com parafuso;

– Ajuste da força de sustentação com arruelas de pressão, parafusos

e furos oblongos;

– Manípulo de ajuste de fim de curso do movimento;

– Alça

para

movimentação;

Dimensões:

– Sem Pedestal: 335 mm (A) x 160 mm (L) x 80 mm (P);

– Peso: 5 Kg

(incluindo suporte); Tela:

– Tipo LCD TFT com diagonal de 7”;

– Formato widescreen;

– Montado em formato retrato;

– Resolução HD 1024x 600 pixels;

– Brilho 200 cd / m2;

– Contraste de 320:1;

– Tempo de Resposta 10 ms;

– Ângulo de visão horizontal de 130°;

– Ângulo de visão vertical de 130°;
– Interface HDMI;
– Backlight em LED;
– Tela de toque:
– Embutido na tela;
– Tecnologia PCAP (capacitivo);
– Ativação da detecção de toque pelo dedo da mão ou outros dispositivos;
– Resistência da superfície >= 6H;
– Transparência > 82%;
– Interface USB;
– Erro máximo de 6 mm (menos de 1,5%);
– Tempo de resposta menor que 10 ms;
– Nível de transparência maior que 85%; Leitor Reconhecimento Facial:
– 1 (uma) Câmera 1.3 MP RGB;
– 1 (uma) Câmera 1.3 MP infravermelho (IR);
– Live detection (não permite uso de foto ou vídeo em meio físico ou digital);
– Capacidade armazenamento mínimo 20.000 usuários;
– Interface Ethernet TCP/IP 10/100/1000 e WiFi;
– Tempo de verificação e liberação de acesso < 0,3 segundo;
– Distância de detecção: ajustável, via software, de 0,3 metro a 4 metros;
– Precisão > 99,9% (1:N);
– Baixo índice de falsa rejeição (FAR 0,01);
– Detecção de presença através de movimentação; Leitor Impressão Digital:
– Leitor óptico com área de captura de 15,24 x 20,32 mm;
– Sensor óptico IP65 FAP 20 compacto;
– Resolução de 500 DPI;
– Imagem de 300 x 400 pixels;

– Reconhecimento mesmo com rotação de 360 graus;
– Tecnologia Multi Dynamic Range (MDR);
– Operação até 100,000 lux;
– Tecnologia Live Fingerprint Detection (LFD);
– Criptografia AES-256;
– FRR= 0,1%;
– FAR= 0,001%;
– Reconhecimento direto com templates/minucias em formato ANSI 378;
– Tempo para reconhecimento 1:1 (10.000 templates) menor que 600 ms;
– Tempo para reconhecimento 1:n (10.000 templates) menor que 1.500 ms;
– Tempo para captura de imagem e extração de template menor que 200 ms;
– Interface de comunicação serial TTL (outras interfaces sob consulta);
– Alimentação DC 5 V, corrente máxima 220 mA; Indicador de LEDs RGB:
– Para indicar Acesso Permitido ou Acesso Negado;
– Composto por 4 (quatro) LEDs RGB SMD 5050;
– Alimentação DC 12-15 V;
– Protegido por policarbonato transparente de 3 mm; Altofalante:
– Para mensagem de voz;
– Com blindagem magnética;
– Potência de 0,25 W;
Buzzer:
– Para indicar Acesso Permitido ou Acesso Negado:
– Tipo contínuo com oscilador interno de 3-30 V DC;
– Nível de pressão sonora 80 DB;
– Dimensões: 35 mm de diâmetro por 20 mm de altura; Fonte de alimentação AC / DC:
– Entrada full range AC 100-240 V 50-60 Hz;

– Saída: DC 15 V / 5 A; Bateria:
– Tipo chumbo ácido selada;
– 12 V / 4 Ah;
– Autonomia para 2 (duas) horas; Controle Eletrônico (CPU):
– Placa CPU que faz o controle dos leitores, LEDs, displays e a comunicação com o HOST;
– Permite atualização do firmware em campo, conectado notebook a CPU, ou remoto;
– Interface Ethernet 10/100 Mbits;
– Comunicação com servidor/HOST via protocolo TCP/IP usando uma porta UDP; Alimentação:
– Entrada para fonte de alimentação DC 12-15 V;
– Entrada para bateria chumbo selada 12 V;
– Chaveamento automático entre as fontes de energia;
– Medidor de nível de bateria e circuito automático carregador de bateria; Interface para leitores:
– Interface serial TTL para leitor de de impressão digital;
– Interface para Display LCD;
– Interface para Display TFT; Sinal sonoro:
– Acionado para indicar acesso liberado;
– Acionado para indicar acesso negado;
– Interface para LEDs;
– Para controle dos LEDs indicadores RGB;
Parâmetros de funcionamento (ajustados localmente ou remotamente via software):
– IP Local, IP do HOST, Porta UDP Local, Porta UDP HOST, Máscara de rede;

– Tentativas para entrada em modo offline;

– Tempo para controle de fluxo (segundos);

– Relógio interno ;

Operação Offline:

– Capacidade de armazenar até 130.000 códigos de acesso;

– Capacidade de armazenar até 130.000 LOGs para códigos de acesso; Opções de configuração do Dispositivo de Reconhecimento Facial:

– companyName: Nome da empresa;

– identifyDistance: Distância em que o dispositivo irá tentar identificar uma pessoa;

– identifyScores: Define qual a taxa de acerto para reconhecer uma pessoa;

– saveIdentifyTime: Define quantos segundos o dispositivo vai aguardar para identificar a mesma pessoa novamente;

– ttsModType: Define se vai falar o nome da pessoa ao reconhece-lá;

– ttsModContent : Define o que vai ser dito quando reconhecer uma pessoa, o reconhecimento fa- cial reconhece as palavras {name} e {temperature};

– displayModType : Mostra os dados de identificação na tela após reconhecer uma pessoa;

– displayModContent: Define o que vai ser mostrado na tela, ao usar a palavra {name} irá mostrar o último nome da pessoa;

– recStrangerType: Define o que fazer caso não reconheça a pessoa; recStrangerTimesThreshold : Define qual o nível de testes usados para identificar uma pessoa, quanto maior o número, mais demorado será o reconhecimento; ttsModStrangerType: Define se o reconhecimento facial irá falar que é uma pessoa não reconhecida;

ttsModStrangerContent: Fala o que tiver escrito podendo ser utilizado a variável {temperature}

Exemplo: "Stranger alert custom";

– multiplayerDetection : Detecta uma ou mais faces na tela;

– Reiniciar Dispositivo;

– Configurar Data/Hora conforme horário do servidor;

– Configurar senha do dispositivo;

– Configurar Logo;

– Configurar Host Server para função de callback dos logs do reconhecimento facial;

– Permissões de acesso (permite escolher quais grupos ou usuários tem acesso ao registro);

– Comandos Para Controle dos Dispositivos (Validadores de Acesso):

– Exibe uma lista com os Dispositivos, Endereço IP, Descrição, Tipo, Sentido de Operação;

– Permite editar informações do dispositivo;

– Permite excluir dispositivo;

– Permite enviar Códigos de Acesso (Modo Offline Manual) para o Dispositivo;

– Verifica se dispositivo está online;

– Carrega informações do dispositivo; Relatório de Acesso:

– Exibe uma lista com um relatório de todos os acessos realizados no evento;

– Exibe Descrição do Evento, Tipo de Acesso, Sequêncial e Nome da Pessoa;

– Permite excluir registros;

– Permite editar os dados associados ao Código de Acesso (Cadastro Pessoa);

– Permite associar outra pessoa ao Código de Acesso;

– Permite bloquear a pessoa associada ao Código de Acesso;

– Permite exportar para arquivo em formato CSV (pode ser aberto diretamente em aplicativo de planilha eletrônica sem nenhum tipo de conversão);

Controle de Empresas, Grupos, Entidades:

– Finalidade de agrupamento das pessoas que são cadastradas no sistema;

– Para agilizar a permissão ou restrição de acessos, relatórios, bloqueios, inserção em eventos, etc;

– Também permite diferenciar grupos de acesso como direção, serviços, etc;

– Nome da Empresa (Grupo ou Entidade);

– Mensagens personalizadas (LOCAL correto, mensagem de boas-vindas);

– Regras de Acesso (LOCAL que pode usar para o acesso);

– Permissões de acesso (permite escolher quais grupos ou usuários tem acesso ao evento);

Comandos para Controle de Empresas, Grupos, Entidades:

– Exibe uma lista com Nome da Empresa, Quantidade de pessoas associadas a empresa, Mensagens personalizadas (Local correto, mensagem de boas-vindas), Regras de Acesso;

– Permite editar as informações da empresa;

– Permite excluir a empresa;

– Permite listar todas as pessoas associadas a empresa;

– Permite adicionar as pessoas associadas a empresa a um determinado evento;

– Permite importar a partir de um arquivo-texto uma lista de pessoas no formato:

Controle de Pessoas:

– Nome da empresa, grupo ou entidade a qual está associada;

– Nome da pessoa;

– Número do documento (RG, CPF, etc);

– Código de acesso (ID do smartcard, código de barras);

– Email;

– Permite visualizar e capturar imagem de pessoas no cadastro (Foto / Webcam);

– Impressão Digital de até 10 (dez) dedos;

– Pode operar em modo de validação 1:N ou 1:1 (código de acesso + finger);

– Prazo de validade (data de expiração) do acesso da pessoa;

– Foto;

– Regras de acesso para a pessoa;

– Permissões de acesso (permite escolher quais grupos ou usuários tem acesso ao registro);

– Comandos para Controle de Pessoas:

– Exibe uma lista com o Nome da Pessoa, Número do Documento, Código de Acesso, Nome da Empresa e Status (Liberada ou Bloqueada);

– Permite editar as informações da pessoa;

– Permite excluir uma pessoa;

– Permite listar o LOGs de acesso nos eventos de uma pessoa;

– Permite bloquear ou liberar uma pessoa;

– Permite adicionar uma pessoa a um determinado evento;

– Permite listar todas as pessoas bloqueados cadastradas no sistema;

– Permite exportar a lista de pessoas cadastradas no sistema para arquivo em formato CSV (pode ser aberto diretamente em aplicativo de planilha eletrônica sem nenhum tipo de conversão);

– Permite imprimir a lista de pessoas cadastradas no sistema;

– Permite testar a imagem da foto no dispositivo;

– Controle de Intervalo de Horários e Dia da Semana:

– Para definição de intervalo de horários em determinado dia da semana;

– Nome (Descrição/Identificador) do horário;

– Dia da Semana;

– Horário de início do intervalo;

– Horário de término do intervalo;

– Permissões de acesso (permite escolher quais grupos ou usuários tem acesso ao evento);

– Permite controlar turnos, jornadas de trabalho por dia e horários;

– Comando Para Controle de Intervalo de Horários e Dia da Semana:

– Exibe uma lista com os Intervalos de Horários e Dia da Semana;

– Permite editar Intervalos de Horários e Dia da Semana;

– Permite excluir Intervalos de Horários e Dia da Semana; Controle de Mensagens nos Validadores:

– Permite personalizar as mensagens que são exibidas nos validadores de acesso;

– Conforme os eventos que acontecem no sistema:

– Acesso permitido;

– Acesso negado;

– Timeout de acesso;

– Algumas mensagens podem usar variáveis como exibir o nome da pessoa no acesso ({nome}), os portões corretos de acesso ({portoes}) e outros;

– Comando Para Controle de Mensagens nos Validadores:

– Exibe uma lista com as Mensagens de Acesso;

– Permite editar uma Mensagem de Acesso;

– Permite excluir uma Mensagem de Acesso;

6. Painel de LED P3.91;

PAINEL PLENÁRIO, PLENARINHO E OUTROS:

Consiste no fornecimento, instalação, configuração e comissionamento de Painel de LED Indoor modelo P3.91, composto por módulos de LED de 64x64 pixels (250x250 mm), com manutenção frontal, pixels formados por LEDs SMD2020

(3-em-1) e características espectrais de alta performance — Vermelho 620–625 nm (690–900 mcd), Verde 518–523 nm (760–860 mcd) e Azul 466–471 nm (420–545 mcd) — incluindo todos os acessórios, estruturas, controladores, fontes de alimentação, cabeamento, testes operacionais e garantia técnica, de forma a fornecer solução completa e plenamente funcional para exibição de imagens, vídeos e conteúdos digitais em ambiente interno.

LEDs:

- P3.91 INDOOR;
- Manutenção frontal;
- Cada pixel é formado por 1 LED SMD2020 (3-em-1);
- Vermelho 620-625 nm; 690-900 mcd;
- Verde 518-523 nm; 760-860 mcd;
- Azul 466-471 nm; 420-545 mcd;
- Módulo de LEDs 64x64 pixels (250x250mm);
- Fixação magnética

por imãs; GABINETE:

- Aço carbono com pintura epóxi preto;
- Manutenção frontal;
- Módulo montados com acoplamento magnético;
- 1.000 mm (L) x 500 mm (A) x 150 mm (P);
- Peso: 20 kg;
- Resolução: 256 (L) x 128 (A) pixels;
- IP31;
- Potência Máxima: 600 W/m2 (para dimensionamento dos cabos e disjuntores);
- Consumo Médio: 180 W/m2 (para estimativa de consumo elétrico);
- Pintura eletrostática com tintura epóxi a pó poliéster microtexturizada com camada média de 60 micra, resistente à exposição dos raios ultravioletas;

- Pintura com certificado de reconhecimento de competência técnica conforme norma NBR ISO/IEC 17025:2005 com realização satisfatória dos ensaios previstos nas normas técnicas, referente a pintura aplicada nas superfícies metálicas constituintes do equipamento como requisito mínimo de qualidade conforme segue:

I. ABNT NBR 11003:2009 – Tintas/Determinação de Aderência. Parâmetro: grau máximo Gr 1 (X1/Y1);

II. ABNT NBR 10443:2008 – Tintas e vernizes/Determinação da espessura da película seca sobre superfícies rugosas (equivalente ASTM D1186-01). Parâmetro: mínimo 50/60 micrômetros filme seco;

III. ABNT NBR 8094:1983 – Material metálico revestido e não revestido/Corrosão por exposição à névoa salina – sem alteração mínimo 300 horas (ausência de corrosão F0 e empolamento d0/t0);

IV. ABNT NBR 8095:1983 – Material metálico revestido e não revestido/Corrosão por exposição à atmosfera úmida saturada – sem alteração mínimo 300 horas (ausência de corrosão F0 e empolamento d0/t0);

V. ABNT NBR ISO 4628-3:2015 - Tintas e vernizes - avaliação da degradação de revestimento - Designação da quantidade e tamanho dos defeitos e da intensidade de mudanças uniformes na aparência - parte 3: Grau de enferrujamento máximo Ri 1 - área com corrosão aflorante limitada a 0,05%;

VI. ABNT NBR 5841:2015 – Determinação do grau de empolamento de superfícies pintadas (equivalente ASTM D714-02). Parâmetro: grau d0 e t0 – isento de bolhas;

VII. ABNT NBR 8754:1985 – Corpos-de-prova revestidos e expostos a ambientes corrosivos/Migração Subcutânea (equivalente ASTM D1654-08). Parâmetro: migração subcutânea máxima de 1 mm;

VIII. ASTM D4060-10 – Standard test method for abrasion resistance of organic coatings by the taber abraser. Parâmetro: índice de perda de material máximo de 20,5 mg para 1000 ciclos;

IX. ASTM D3359-09 – Standard test methods for measuring adhesion by tape test (método a). Parâmetro: mínimo 4A – impacto reversivo 1/16" sem perda de adesão;

X. ASTM D3363-05 - Standard test method for film hardeness by pencil test. Parâmetro: apresentando um valor mínimo de 5H ou mais duro.

PAINEL:

- Brilho: 1.200 NITs;
- Ajuste de brilho por software de 16 bits;
- Processamento de cor de 24 bits;
- 280 trilhões de cores;
- Escala de cinza: 12 bits;
- Refresh Rate: 1920 Hz;
- Scan: 1/16;

- Vida útil 100.000 horas;
- Ângulo Vertical +/- 70 graus;
- Ângulo Horizontal +/- 70 graus;
- Temperatura de operação -20 Celsius a +65 Celsius; ALIMENTAÇÃO:
- Entrada 110/220 V com chaveamento manual;
- 60 Hz;

ESTRUTURA:

Fixação em parede;

- Suportes para fixação dos gabinetes na parede;
- Bordas em preto;
- Projeto composto de peças de adequação para fixação dos gabinetes fabricadas em açocarbono com pintura epóxi preto fosco;
- Pintura eletrostática com tintura epóxi a pó poliéster microtexturizada com camada média de 60 micra, resistente à exposição dos raios ultravioletas;
- Pintura com certificado de reconhecimento de competência técnica conforme norma NBR ISO/IEC 17025:2005 com realização satisfatória dos ensaios previstos nas normas técnicas, referente a pintura aplicada nas superfícies metálicas constituintes do equipamento como requisito mínimo de qualidade conforme segue:

I. ABNT NBR 11003:2009 – Tintas/Determinação de Aderência. Parâmetro: grau máximo Gr 1 (X1/Y1);

II. ABNT NBR 10443:2008 – Tintas e vernizes/Determinação da espessura da película seca sobre superfícies rugosas (equivalente ASTM D1186-01). Parâmetro: mínimo 50/60 micrômetros filme seco;

III. ABNT NBR 8094:1983 – Material metálico revestido e não revestido/Corrosão por exposição à névoa salina – sem alteração mínimo 300 horas (ausência de corrosão F0 e empolamento d0/t0);

IV. ABNT NBR 8095:1983 – Material metálico revestido e não revestido/Corrosão por exposição à atmosfera úmida saturada – sem alteração mínimo 300 horas (ausência de corrosão F0 e empolamento d0/t0);

V. ABNT NBR ISO 4628-3:2015 - Tintas e vernizes - avaliação da degradação de revestimento - Designação da quantidade e tamanho dos defeitos e da intensidade de mudanças uniformes na aparência - parte 3: Grau de

enferrujamento máximo Ri 1 - área com corrosão aflorante limitada a 0,05%;

VI. ABNT NBR 5841:2015 – Determinação do grau de empolamento de superfícies pintadas (equivalente ASTM D714-02). Parâmetro: grau d0 e t0 – isento de bolhas;

VII. ABNT NBR 8754:1985 – Corpos-de-prova revestidos e expostos a ambientes corrosivos/Migração Subcutânea (equivalente ASTM D1654-08). Parâmetro: migração subcutânea máxima de 1 mm;

VIII. ASTM D4060-10 – Standard test method for abrasion resistance of organic coatings by the taber abraser. Parâmetro: índice de perda de material máximo de 20,5 mg para 1000 ciclos;

IX. ASTM D3359-09 – Standard test methods for measuring adhesion by tape test (método a). Parâmetro: mínimo 4A – impacto reversivo 1/16" sem perda de adesão;

X. ASTM D3363-05 - Standard test method for film hardeness by pencil test. Parâmetro: apresentando um valor mínimo de 5H ou mais duro.

Plataforma gerenciadora:

- Software com exibição de vários formatos de mídia como BMP, JPG, GIF, PCX, MPG, MPEG, MPV, MPA, AVI, VCD, SWF, RM, RA, RMJ e ASF e outros;
- Controlador que recebe o sinal de vídeo DVI e distribui para os gabinetes através de cabo de rede UTP Cat 6e;
- Ajuste manual e pré-agendamento de luminosidade;
- Ajuste manual de contraste, saturação e todas as funcionalidades para qualificação de imagens.
- Hardware plataforma gerenciadora:

Equipamento com configuração similar ou superior a NOTEBOOK 15.6” 16GB SSD 512GB W11P.

VIDEO PROCESSOR:

- Função PIP (Picture-In-Picture);
- Função Multi Windows (Mosaic) para exibir diferentes origens de vídeo no PFC;
- Entradas: 4xHDMI 2.0; 2xDP1.2; 2xHDMI 1.3; 2x3G-SDI; 2xCVBS;

7 Postos de votação com reconhecimento facial para votação e presença;

Os Postos de Votação com Reconhecimento Facial constituem uma estação autônoma de autenticação biométrica e captura de votos, projetada para operar em ambientes legislativos, corporativos e institucionais. O sistema é composto por um conjunto integrado de hardware embarcado, algoritmos avançados de biometria facial, módulos criptográficos, software de votação e comunicação segura com a plataforma central de governança dos votos e atas digitais.

7.1. Estrutura de Hardware do Posto de Votação

DA SOLUÇÃO DO SISTEMA AUTOMATIZADO ACOPLADO EM MESA, COMPOSTO DE (SUPORTE AUTOMATIZADO, SOFTWARE APLICATIVO PARA INSTALAÇÃO DE TABLET):

A caixa em relação a moldura (estática) possibilitará um giro de 90° e, quando o mesmo tiver na posição de 0° ele estará fechado e rente com o plano da mesa. Quando ele der o giro de 90°,

ele estará na vertical, posição de operação e em ângulo (para o Parlamentar) em relação ao plano da mesa, conforme pode ser visto nas figuras do Edital. Esta possibilidade de abertura só será realizada por pessoas que possuem o aplicativo para esta operação, tornando o terminal anti-vandalismo e tecnologicamente seguro.

A solução será desenvolvida e personalizada para a Câmara Municipal do Recife, bem como será entregue, instalada e configurada para o seu pleno uso.

ESTRUTURA DE COMPOSIÇÃO DA "SOLUÇÃO AUTOMATIZADA"

ESTRUTURA:

- Em chapas de aço inox escovado;
- Eixo para movimentação (giro) do tablet;
- Motor para automatizar abertura e fechamento;
- Botão, fixado no tampo, para acionamento do motor;
- Sensor de corrente para evitar esmagamento

e superaquecimento; FIXAÇÃO DO TABLET:

- Colado na chapa de aço inox;
- Suporte de fixação na chapa de aço inox;
- Tablet na posição vertical/horizontal (a ser escolhido

no local); CAIXA DE TOMADAS:

- 1x Tomada 2P + T 10A;
- 1x

Tomada USB;

FONTE

ALIMENTAÇÃO:

- Entrada: Full Range 100-240 V AC 50-60 Hz;
- Saída: 12 V / 5 A;
- Fixada embaixo do tampo

da mesa; ALIMENTAÇÃO USB:

- Conversor DC-DC 0,8 A alimentado pela Fonte 12 V

/ 5 A; CONTROLE DO MOTOR:

- Microcontrolado;
- Acionamento PWM;
- Sensor de Corrente para controle de esmagamento;
- Sensor de posição da rotação;
- Wi-Fi para interface com Aplicativo

APK; FECHAMENTO DA ABERTURA TERMINAL

ANTERIOR:

- Tampo de fechamento quando terminal anterior for retirado
- Em chapas de aço

inox escovado; INSTALAÇÃO:

- Recorte no tampo da mesa;
- Fresagem para embuitr a chapa de inox no tampo, deixando tampo

da mesa e chapa de inox na mesma altura (sem degrau);

CARACTERÍSTICAS DA ESTRUTURA

- Material: chapas de aço inox escovado AISI 304 de 1,2 e 1,5mm de espessura;
- Pinos capacitivos: padrão métrico PEM;
- Parafusos e porcas: sistema métrico;
- Processos: corte laser, dobras em máquina CNC, solda MIG/MAG

e descarga capacitiva, rebarbamento, lixação e escovação;

LEITOR BIOMÉTRICO DE IMPRESSÃO DIGITAL

- Sensor óptico;- Auto on (auto captura);
- LFD (Live Finger Detection);
- FRR 0.1 %;- FAR 0.001%;
- Interface

serial TTL;

POSICIONAMENTO

:

- Dentro da área que acondiciona o tablet (não ficará visível quando estar fechado);
- Ficará para dentro da estrutura de aço inox; TECLADO PARA VOTAÇÃO:
- Interruptor do tipo mecânico com "keycap" para melhor conforto/precisão ao teclar;
- Teclas em plástico ABS injetado;
- Dimensões da área de toque: 14 mm * 24 mm;
- Tecla SIM: injetada na cor verde;- Tecla NÃO: injetada na cor vermelha;
- Tecla ABSTENÇÃO: injetada na cor amarela; POSICIONAMENTO:
- Dentro da área que acondiciona o tablet (não ficará visível quando estar fechado);
- Ficará para dentro da estrutura de aço inox; MIDDLEWARE PARA FINGERPRINT:

Middleware (MW):

- Windows;
- Interface SV: IP (chamadas HTTP/JSON);
- Interface Leitor Biométrico: IP / UDP Criptografado / WiFi;
- Cadastro dos leitores biométricos: IP;
- Cadastro do leitor biométrico de cadastramento de parlamentares;
- Banco de dados com os templates de impressão digital;
- Motor de operação/comunicação UDP Criptografada/WiFi com os leitores biométricos;

TABLET

Especificações Mínimas

Processador:

Velocidade do Processador: 2.3GHz, 1.7GHz

Tipo de Processador: Octa Core

Tela

Tela: Tamanho (Tela Principal): 10.4" (263.1mm)

Resolução (Tela Principal): 2000 x 1200 (WUXGA+)

Tecnologia (Tela Principal): TFT

Profundidade de Cor (Tela Principal): 16M

Câmera: ✦ Câmera Traseira - Resolução: 8.0 MP

Câmeras Traseiras - Foco Automático: Sim

Câmera Frontal - Resolução: 5.0MP

Resolução de Gravação de Vídeos: FHD (1920 x 1080) @30fps

Memória: ✦ Memória RAM (GB): 4 GB

Memória Total Interna (GB): 64 GB

Memória Disponível (GB): 49.2 GB

Suporte ao Cartão de Memória: MicroSD (até 1TB)

Rede / Bandas: 2G GSM: GSM 850, GSM ✦ 900, DCS 1800, PCS1900 ✦ 3G UMTS:

B1 (2100), B2

(1900), B4 (AWS), B5 (850), B8 (900) ✦ 4G FDD LTE: B1 (2100), B2 (1900), B3

(1800), B4 (AWS), B5 (850), B7 (2600), B8 (900), B12 (700), B17 (700), B20 (800), B28 (700), B66(AWS-3) 4G TDD
LTE: B38 (2600), B40 (2300) ✦

Conectividade:

ANT+: Sim

USB 2.0

Localização: GPS, Glonass, Beidou, Galileo

Conector de Fone de Ouvido: Conexão 3.5mm Estéreo (Padrão

P2) Wi-Fi: 802.11 a/b/g/n/ac 2.4G+5GHz, VHT80 MIMO

Wi-Fi Direct: Sim

Versão de Bluetooth: Bluetooth v5.0 (LE até 2 Mbps)

NFC: Não

Perfis de Bluetooth: A2DP, AVRCP, DI, HFP, HID, HOGP, HSP, MAP, OPP, PAN, PBAP

PC Sync: Smart Switch (Versão para PC)

Sistema Operacional:

Android

Informações

Gerais:

Formato:

Tablet Cor:

Cinza Caneta

Sensores:

Acelerômetro, Giroscópio, Sensor de Efeito Hall, Sensor de Luz RGB

Especificações Físicas:

Dimensões (AxLxP, mm): 244.5 x 154.3 x 7.0

Peso (g): 467

Bateria:

Uso de internet 4G (Horas): até 12
Uso de Internet Wi-Fi (Horas): até 12 Reprodução de Vídeos (Horas): até 13
Capacidade da Bateria (mAh, Typical): 7040 Bateria removível: Não
Tempo de Reprodução de Áudio (Horas): até

149 Tempo em ligações (3G WCDMA) (Horas):

até 39 Carregador

Cabo USB

Áudio e Vídeo:

Formato de Reprodução de Vídeo: MP4, M4V, 3GP, 3G2, WMV, ASF, AVI, FLV, MKV, WEBM

Resolução de Reprodução de Vídeo: UHD 4K (3840 x 2160)@120fps

Formato de Reprodução de Áudio: MP3, M4A, 3GA, AAC, OGG, OGA, WAV, WMA, AMR,AWB, FLAC, MID, MIDI, XMF, MXMF, IMY, RTTTL, RTX, OTA

Reconhecimento facial: O equipamento deve realizar o reconhecimento facial dos vereadores no aplicativo/sistema de painel eletrônico desta Casa Legislativa.

7.3. Software do Posto de Votação

7.3.1. Aplicação de

Votação Inclui interface

responsiva com:

Exibição de pautas e matérias a serem votadas;

Botões de escolha (Sim/Não/Abstenção) ou opções parametrizadas;

Registro automático de presença ao validar a biometria;

Bloqueio automático após voto computado.

7.3.2. Motor de Criptografia e

Auditoria O sistema utiliza

criptografia fim-a-fim:

AES-256 para dados em repouso;

TLS 1.3 para dados em trânsito;

Assinaturas digitais via RSA-4096 ou Elliptic Curve P-256;
Registro imutável dos votos em ledger distribuído (blockchain privado opcional);
Carimbo de tempo (timestamp trusted) por NTP seguro.

7.3.3. Arquitetura de Comunicação

Protocolo MQTT ou HTTPS com compressão GZIP;

Mecanismo de fallback para comunicação offline com sincronização posterior;

Monitoramento contínuo por heartbeat (intervalo 5 s).

7.3.4. Gestão de Perfis e Controle de Acesso

Acesso administrativo apenas com autenticação multifatorial;

Perfis segregados: Operador, Técnico de TI, Auditor, Gestor;

Logs independentes para trilha de auditoria.

7.4. Mecanismos de Segurança Física e Lógica

7.4.1. Segurança

Física Vedação IP40 ou

superior;

Fechaduras com chave antifurto;

Lacres invioláveis com numeração seriada;

Sensor anti-intrusão que desativa o módulo biométrico ao abrir o gabinete.

7.4.2. Segurança

Lógica Boot seguro

(Secure Boot);

Assinatura digital do firmware;

Whitelist de aplicações permitidas;

Detecção de root e integridade do sistema operacional via checksums SHA-256.

7.5. Integração ao Sistema Central de Governança da Votação

O posto integra-se nativamente a um ecossistema centralizado composto por:

Servidor de votação (orquestração, autenticidade e consolidação dos votos);

Servidor biométrico (templates faciais e validação);

Dashboard administrativo com supervisão em tempo real;

API RESTful e WebSockets para comunicação com painéis de plenário, painéis

públicos e sistemas de presença;

Integração com terminal de autoatendimento, aplicativo mobile de votação e painel full color para plenário.

7.6. Funcionalidades Operacionais do Posto

Identificação automática ao se aproximar do sensor (face tracking + face detection);

Registro imediato de presença ao validar a biometria;

Liberação da interface de votação somente após autenticação facial bem-sucedida;

Emissão de alertas para inconsistências biométricas;

Suporte a múltiplos idiomas;

Relatórios de utilização, presença e disponibilidade em tempo real.

7.7. Conformidade Normativa e Padrões Técnicos O sistema segue:

LGPD – Lei Geral de Proteção de Dados;

Normas ISO/IEC 27.001

8. Super APP:

Desenvolvimento do Super App para Câmara Municipal do Recife. A licitante deverá ter capacidade de desenvolvimento de software para projetar, desenvolver, implantar e manter um Super Aplicativo Mobile e Web destinado ao atendimento legislativo e à comunidade, reunindo em uma única plataforma funcionalidades de transparência, participação popular, serviços ao cidadão, comunicação institucional e suporte às atividades dos vereadores e servidores da Câmara Municipal do Recife.

JUSTIFICATIVA

O desenvolvimento do Super App visa:

Modernizar e digitalizar os serviços da Câmara Municipal.

Aprimorar a transparência e o acesso às informações legislativas.

Facilitar a comunicação entre cidadãos, vereadores e servidores.

Centralizar serviços públicos em plataforma única.

Reduzir atendimentos presenciais e aprimorar a gestão interna.

Estimular a participação popular nas decisões legislativas.

ESCOPO DOS SERVIÇOS

Desenvolvimento e Entrega do Super App

A contratada deverá entregar um aplicativo completo, contemplando:

Aplicativo Mobile (iOS e Android)

Aplicativo nativo ou híbrido de alta performance.

Publicação nas lojas (App Store e Google Play).

Push notifications e personalização por perfil.

Versão Web Responsiva

Portal web com as mesmas funcionalidades essenciais do app.

Painel Administrativo (Backoffice)

Gerenciamento de conteúdo, serviços, permissões e indicadores.

Estatísticas e dashboards de uso.

Funcionalidades Obrigatórias

A) Transparência e Atividade Legislativa

Consulta de Projetos de Lei, Requerimentos, Pareceres e Votações.

Acompanhamento do trâmite legislativo em tempo real.

Sessões plenárias:

Transmissão ao vivo,

Gravações,

Agenda do Legislativo.

Perfil completo dos vereadores.

B) Participação Popular

Ouvidoria Digital integrada (protocolo e acompanhamento).

Enquetes legislativas e consultas públicas.

Votação cidadã por bairro/tema.
Chatbot com respostas rápidas e automáticas. Canal "Fale com Seu Vereador".
C) Serviços ao Cidadão

Agendamento de visitas, audiências e atendimentos.

Acesso a documentos e certidões.

Agenda de eventos da Câmara.

Mapa de serviços municipais (quando aplicável).

D) Área Exclusiva do Vereador

Recebimento de demandas dos

cidadãos. Gestão do gabinete via

app.

Publicação de atividades, agendas e comunicados.

Ferramentas de comunicação com a comunidade.

E) Área do Servidor

Acesso a documentos internos.

Solicitações administrativas.

Reserva de salas.

Comunicação
interna.

F) Recursos Avançados

Autenticação GovBR (obrigatória).

Geolocalização por

bairros/regiões.

Acessibilidade completa (Libras, alto contraste, leitor de tela).

Motor de personalização por perfil de usuário.

Design e UX

Interface moderna, responsiva e intuitiva.

Componentes acessíveis conforme WCAG 2.1

AA.

Protótipos (wireframes + mockups) deverão ser aprovados pela Câmara.

Integrações Obrigatórias

A contratada deverá integrar o Super App aos seguintes sistemas:
Sistema de Processo Legislativo da Câmara. Serviço de Ouvidoria (e-Ouv ou equivalente). Redes sociais oficiais.
Mecanismos GovBR (login e validação).

APIs da Prefeitura (quando aplicável).

A contratada deverá desenvolver APIs próprias quando necessário.

Segurança e LGPD

O sistema deve atender:

LGPD (Lei nº 13.709/2018).

Criptografia em repouso e em trânsito (TLS 1.2+).

Políticas de backup e recuperação.

Logs e auditoria de acessos.

Gestão de perfis e permissões.

Entregas Esperadas

Documento de levantamento de requisitos.

Protótipos navegáveis (Figma ou similar).

Aplicativo iOS e Android publicados.

Portal Web responsivo.

Painel Administrativo.

Documentação técnica completa.

Treinamento para servidores e gabinetes.

Suporte e manutenção pós-implantação.

PRAZOS

Início do projeto: após assinatura do contrato.

Entrega do protótipo: até 30 dias.

Versão beta (testes): até 90 dias.

Versão final e implantação: até 120

dias.

Suporte contínuo: conforme período contratual.

MODELO DE PRESTAÇÃO

A contratação ocorrerá nas modalidades:

Desenvolvimento + Manutenção contínua, e

Software como Serviço (SaaS), incluindo suporte, atualizações e hospedagem.

SUPORTE E MANUTENÇÃO

A contratada deverá fornecer:

Atendimento via e-mail, telefone e sistema de chamados.

Correções de erros em até 48h.

Atualizações evolutivas, corretivas e de segurança.

Monitoramento contínuo da aplicação.

SLA – Níveis de Serviço Mínimos

Disponibilidade da solução: 99% mensal.

Chamados críticos: resposta em até 2 horas.

Chamados de média prioridade: até 8 horas.

Chamados de baixa prioridade: até 48 horas.

CRITÉRIOS DE ACEITAÇÃO

Validação de todas as funcionalidades previstas.

Aprovação de testes funcionais, de carga e segurança.

Publicação nas lojas.

Treinamento e entrega de documentação.

REQUISITOS TÉCNICOS

Arquitetura escalável (cloud preferencial).

Linguagens e frameworks modernos (React Native, Flutter ou equivalentes).

API REST ou GraphQL.

Banco de dados relacional ou NoSQL de alta disponibilidade.

Conformidade com padrões de segurança OWASP.

AMBIENTE TECNOLÓGICO EM NUVEM SOLUÇÃO DE ONBOARDING FACIAL
Solução de onboarding facial via API, com o intuito de otimizar o processo de validação de identidade e garantir segurança e eficiência no gerenciamento de acessos.
A solução a ser contratada deverá atender aos seguintes requisitos:

Experiência do Usuário:

Jornada de Onboarding: O onboarding facial deverá ser realizado em cerca de 01 minuto.

Onboarding Transparente: A solução deverá permitir um login transparente e sem fricção, iniciado a partir do ambiente existente do usuário.

Integração: A solução deve ser capaz de se conectar aos sistemas de ticketing, aplicativos ou outros ambientes sem a necessidade de troca de sistema.

Feedback de Status: A solução deverá fornecer feedback claro e em tempo real durante a captura, incluindo informações sobre o status da validação facial (foto aprovada, em aprovação, reprovada com motivo, etc.).

Envio de Link para Captura: A solução deverá permitir o envio de um link para captura da foto via e-mail, WhatsApp ou compartilhamento de link.

Ajuste nos Requisitos de Foto: Os requisitos da foto deverão ser ajustáveis conforme o hardware de reconhecimento facial existente.

Validação Rápida: A solução deve validar e liberar o acesso do usuário em até 02 segundos.

Reconhecimento de Gêmeos Idênticos: A solução deverá incluir uma funcionalidade para reconhecimento de gêmeos idênticos sem fricção no momento do acesso.

Tecnologia e Desempenho

. Captura Automática de Biometria Facial: A solução deverá realizar a captura automática da biometria facial.

Captura de Documentos: A solução deverá permitir a captura de documentos com foto e identificar o tipo do documento (CNH, RG, Passaporte, Certidão de Nascimento, etc.).

Validação Facial 3D: A solução deve realizar validação biométrica facial 3D ultrarrápida com liveliness (prova de vida).

Detecção de Fraudes: A solução deverá detectar e impedir fraudes digitais, como fotos ou vídeos manipulados (deepfake).

Otimização de Imagens: As imagens deverão ser otimizadas para redução de até 17Kb no banco de dados.

Validação Automática ou Manual: A solução deve permitir validação automática e, em caso de contingência, validação manual.

Painel Forense Inteligente: A solução deverá fornecer um painel forense inteligente com dados e insights para avaliar e cruzar informações do usuário.

Escalabilidade e Nuvem: O onboarding deverá ser realizado em servidores na nuvem, com capacidade de escalar para milhares de capturas simultâneas.

Disponibilidade e Desempenho: A solução deverá garantir uma disponibilidade mínima de 99,99%.

APIs Adaptáveis: A solução deve oferecer APIs que se ajustem às necessidades de diferentes projetos, clientes e cenários.

Calibração de Parâmetros: A solução deverá permitir a calibração dos parâmetros para detectar e alertar sobre óculos, iluminação inadequada, obstruções faciais, entre outros impedimentos.

Certificações: O processo de disponibilidade e desempenho deverá estar alinhado com os parâmetros das normas ISO 9001 e ISO 27001.

Integração e Compatibilidade Compatibilidade Mobile: A solução deverá ser compatível com smartphones Android e iOS, sendo otimizada para captura por selfie ou câmera traseira.

Integração via API: A solução deverá ser integrada via API REST, utilizando apenas dois métodos: GET (consulta de status) e POST (cadastro com retorno da URL do onboarding).

Inteligência Artificial de Reconhecimento: A solução deve utilizar IA própria para reconhecimento e validação facial.

. Integração com Órgãos Federais: A solução deverá integrar-se com APIs de órgãos federais para validação instantânea de documentos.

Alinhamento com LGPD: A solução deve estar em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Segurança e Proteção de Dados

Link de Onboarding Tokenizado: A solução deve gerar links tokenizados e temporários para onboarding facial, com proteção antivazamento.

Armazenamento Seguro: O armazenamento das faciais deverá ser protegido por criptografia e a URL de acesso será temporária.

Adequação à LGPD: A solução deverá estar em total conformidade com a LGPD.

Autorização para Menores: A solução deverá permitir a captura de foto de menores de idade, mediante aceitação de responsabilidade por um responsável maior de idade.

Detecção de Fraudes: A solução deve ser capaz de detectar e impedir documentos falsos, manuscritos ou incompatíveis com a imagem facial capturada.

Detecção de Liveliness e Antideepfake: A solução deve ser capaz de detectar e impedir fraudes no onboarding, incluindo deepfake.

Comunicação e Relatórios

Integração com WhatsApp Business e Outros Meios: A solução deverá permitir a integração com WhatsApp Business, e-mail e SMS para envio de alertas e comunicações em massa.

Relatórios de Validação e Acuracidade: A solução deverá gerar relatórios com motivos de reprovação e índices de acuracidade das validações faciais.

Relatórios de Performance: A solução deve permitir o acompanhamento do percentual de aprovações automáticas versus manuais, e de conclusão do fluxo versus cadastros iniciados.

Relatórios Demográficos: A solução deverá fornecer relatórios demográficos sobre os usuários, incluindo comportamento e hábitos.

Controle de Acessos em Tempo Real: A solução deverá gerar relatórios de controle de acesso em tempo real, com dashboards de acessos por local, pier, catraca, entre outros.

TERMINAL AUTOATENDIMENTO CÂMARA MUNICIPAL DO RECIFE

Gabinete:

Fabricado em chapas de aço carbono de 1,5mm de espessura;

Pintura eletrostática com tintura epóxi a pó poliéster micro texturizada;

Acabamentos do terminal em aço escovado;

Sistema de ventilação forçada com 1 (um) ventilador;

Acesso traseiro para manutenção e operação dos equipamentos;

Porta exclusiva para acesso a operação da impressora e troca de papel;

Dotado de fechaduras TETRA, todas com o mesmo segredo;

A entrada da rede elétrica é independente da entrada da rede lógica;

O cabo de rede de dados é conectado internamente, em conector fixado ao gabinete;

Interruptor externo, com chave com fechadura, para ligar e desligar o terminal;

Sapatas de nivelamento;

Laterais da tampa frontal com policarbonato de acabamento iluminado com LEDs RGB;

Permite a personalização visual;

Dimensões do Terminal com tolerância de 5% para mais ou para menos:

Altura total: 1530 a 1.580mm (incluindo as sapatas de nivelamento); Largura total: 445 a 485mm;
Profundidade do corpo principal: 120 mm;

Profundidade total: 530 a 570mm (incluíndo base e PIN PAD/Leitora RFID);

Peso: 100 kg;

Alimentação:

Full range 100-240 V AC 50-60 Hz;

Disjuntor interno de proteção;

Régua de tomadas, com fusível de proteção;

Potência Máxima: 300 W e Potência Média: 50 W;

Monitor LCD:

Diagonal de 18.5”;

Proporção 16:9 (widescreen), montado em formato paisagem;

Resolução HD 1360 x 768 pixels;

Brilho 250 cd / m2;

Contraste de 400:1;

Tempo de Resposta 8 ms (médio); Ângulo de visão horizontal de 140°; Ângulo de visão vertical de 120°;

Possui controles para ajuste de brilho e contraste;

O conector do cabo de vídeo padrão DB15 VGA;

Alimentação full range AC 100-240V 50-60Hz com ligação automática;

Tela de Toque:

Tecnologia resistiva;

Ativação da detecção de toque pelo dedo da mão (mesmo com o uso de luvas), ou outros dispositivos;

Tela resistente a graxas, óleos, água e outros contaminantes tipo gordura em geral;

Vidro de proteção de espessura de 2mm; Erro máximo de 6mm (menos de 1,5%);

Pelo menos 15.000 (quinze mil) pontos de toque por cm2;

Força de ativação menor que 20g a 80g;

Durabilidade de pelo menos 1 (um) milhão de toques;

Tempo de resposta menor que 10ms;

Nivel de transparência maior que 80%;

Dureza de nível 3 (escala Mohs);

Controlador com interface USB com resolução de 4096 x 4096 touchpoints;

Driver para Windows e Linux;

CPU:

Processador I3;

Memória 8 GB;

SSD 120 GB;

Ethernet 10/100/1000;

Vídeo HDMI;

6 (seis) Portas USB;

WEBCAM 2.0MP

Posicionada acima do monitor, dentro da estrutura do gabinete;

Disponível para os gabinentes:

Características:

2.0 Megapixel (True);

CMOS Sensor;

Captura de imagem: 1600 x 1200 pixels;

Vídeo: 1600 x 1200 pixels @ 15fps MPEG (1600 x 1200 @ 6-8fps YUV);

Até 30 quadros por segundo (resolução 640 x 480 pixels MPEG ou 640 x 480 pixels YUV);

Ângulo: 48º Vertical / 63º Horizontal;
Auto foco (8cm até infinito / F2.8);

Ajustes automáticos sob condições de baixa luminosidade:

Auto White Balance;

Auto Exposure Control;

Microfone interno;

Sem software a ser instalado, nenhuma configuração de recursos é necessária;

Alimentação:

Voltagem: 5VDC (USB);

Consumo máximo: 250mA;

SISTEMA DE SOM

Possui 2 (dois) alto-falantes (saída de som stéreo);

Características Técnicas dos alto-falantes:

Diâmetro de 2”;

Com blindagem magnética;

Potência de 1 (um) Watt;

Circuito amplificador conectado a CPU do terminal;

Conector jack P2 que permite a utilização de fones de ouvido externos;

Superfície circunvizinha côncava para orientar o curso de inserção do conector;

Corte automático do som dos alto-falantes do terminal ao inserir o fone de ouvido;

Controle de volume digital próximo a conector jack P2;

1 (um) botão em plástico ABS com dimensões de 10 x 10mm para aumentar o volume;

1 (um) botão em plástico ABS com dimensões de 10 x 10mm para diminuir o volume;

O ajuste do volume pode ser feito a qualquer momento;

Sinalização tátil com dimensão de 15 mm x 15 mm (NBR15250);

Detecção da conexão do plug do fone de ouvido permitindo que seja acionada software específico;

MONOFONE

O monofone para terminal de autoatendimento deverá ser fornecido como componente integrante da solução, destinado à comunicação de voz entre o usuário do terminal e a central de atendimento, suporte remoto ou sistema de intercomunicação institucional.

Requisitos Funcionais Mínimos

a) Permitir comunicação de voz bidirecional, com qualidade e inteligibilidade adequadas, entre o usuário e o atendente remoto ou sistema integrado;

b) Possibilitar acionamento pelo usuário diretamente no terminal de autoatendimento;

c) Operar de forma contínua, adequada a ambientes de uso público e alto fluxo de pessoas;

d) Possibilitar atendimento assistido, inclusive para usuários com dificuldades operacionais.

Requisitos Técnicos Mínimos

a) Microfone integrado de alta sensibilidade, com recursos de redução ou cancelamento de ruídos ambientais;

b) Alto-falante interno com potência compatível para ambientes com ruído moderado;

c) Sistema de detecção de retirada e reposicionamento do monofone por meio de gancho ou sensor equivalente;

d) Interface de comunicação compatível com o terminal de autoatendimento, podendo ser analógica, digital, VoIP ou proprietária, conforme a solução ofertada;

e) Alimentação elétrica proveniente do próprio terminal ou por meio de fonte dedicada compatível;

f) Cabo de conexão reforçado, com resistência à tração e ao uso contínuo.

Características Construtivas

a) Corpo confeccionado em material de alta resistência mecânica, como ABS, policarbonato ou material equivalente;

b) Design ergonômico, adequado ao uso frequente e prolongado;

c) Construção robusta, apropriada para operação ininterrupta (24x7);

d) Resistência ao desgaste decorrente do uso intensivo em ambientes públicos.

Integração e Compatibilidade

a) Totalmente compatível e integrável aos terminais de autoatendimento e aos sistemas de software utilizados pela CONTRATANTE;

b) Não demandar adaptações estruturais adicionais além das previstas no projeto do terminal;

c) Permitir integração com sistemas de atendimento remoto, interfonia ou plataformas equivalentes.

Condições de Operação

a) Indicado para operação em ambientes internos ou semiabertos;

b) Operar dentro das condições ambientais típicas de equipamentos de uso público;

c) Manter desempenho adequado mesmo em ambientes com níveis elevados de ruído.

Normas e Conformidades

a) Atender às normas técnicas brasileiras aplicáveis, especialmente às relacionadas à segurança elétrica e compatibilidade eletromagnética;

b) Estar em conformidade com os requisitos legais e regulamentares vigentes;

c) Atender, quando aplicável, aos requisitos de acessibilidade.

Versão Web Responsiva Portal web com as mesmas funcionalidades essenciais do app.

Painel Administrativo (Backoffice)

Gerenciamento de conteúdo, serviços, permissões e indicadores.

Estatísticas e dashboards de uso.

Funcionalidades Obrigatórias

A) Transparência e Atividade Legislativa

Consulta de Projetos de Lei, Requerimentos, Pareceres e Votações.

Acompanhamento do trâmite legislativo em tempo real.

Sessões plenárias:

Transmissão ao vivo,

Gravações,

Agenda do Legislativo.

Perfil completo dos vereadores.

B) Participação Popular

Ouvidoria Digital integrada (protocolo e acompanhamento).

Enquetes legislativas e consultas públicas.

Votação cidadã por bairro/tema.

Chatbot com respostas rápidas e automáticas.

Canal "Fale com Seu Vereador".

C) Serviços ao Cidadão

Agendamento de visitas, audiências e atendimentos.

Acesso a documentos e certidões.

Agenda de eventos da Câmara.

Mapa de serviços municipais (quando aplicável).

D) Área Exclusiva do Vereador

Recebimento de demandas dos

cidadãos. Gestão do gabinete via

app.

Publicação de atividades, agendas e comunicados.

Ferramentas de comunicação com a comunidade.

E) Área do Servidor

Acesso a documentos internos.

Solicitações administrativas.

Reserva de salas.

Comunicação
interna.

F) Recursos Avançados

Autenticação GovBR (obrigatória).

Geolocalização por

bairros/regiões.

Acessibilidade completa (Libras, alto contraste, leitor de tela).

Motor de personalização por perfil de usuário.

Design e UX

Interface moderna, responsiva e intuitiva.

Componentes acessíveis conforme WCAG 2.1

AA.

Protótipos (wireframes + mockups) deverão ser aprovados pela Câmara.

Integrações Obrigatórias

A contratada deverá integrar o Super App aos seguintes

sistemas: Sistema de Processo Legislativo da Câmara.

Serviço de Ouvidoria (e-Ouv ou equivalente).

Redes sociais oficiais.

Mecanismos GovBR (login e validação).

APIs da Prefeitura (quando aplicável).

A contratada deverá desenvolver APIs próprias quando necessário.

Segurança e LGPD

O sistema deve atender:

LGPD (Lei nº 13.709/2018).

Criptografia em repouso e em trânsito (TLS 1.2+).

Políticas de backup e recuperação.

Logs e auditoria de acessos.

Gestão de perfis e permissões.

Entregas Esperadas

Documento de levantamento de requisitos.

Protótipos navegáveis (Figma ou similar).

Aplicativo iOS e Android publicados.

Portal Web responsivo.

Painel Administrativo.

Documentação técnica completa.

Treinamento para servidores e gabinetes.

Suporte e manutenção pós-implantação.

DESISNTALAÇAO DO VÍDEO WALL EXISTENTE NO PLENÁRIO ATUAL E REINSTALAÇÃO NOS DEMAIS AMBIENTES DA CASA LEGISLATIVA

O plenário da Casa Legislativa possui atualmente um videowall plenamente operacional, instalado conforme a configuração anterior do ambiente. Todavia, diante da necessidade de reestruturação física e funcional do plenário, bem como da implantação de novas soluções tecnológicas integradas aos sistemas legislativos e audiovisuais, torna-se imprescindível a desinstalação técnica e segura do referido equipamento.

A posterior reinstalação do videowall em outras dependências da Casa Legislativa justifica-se pela otimização do uso dos ativos públicos existentes, pelo aproveitamento integral do investimento previamente realizado e pela adequação do equipamento a ambientes que demandam soluções de visualização de alto impacto, tais como áreas institucionais, salas de apoio, auditórios ou espaços destinados à comunicação e à transparência dos atos legislativos.

A execução desses serviços requer mão de obra especializada, observância às boas práticas de engenharia e normas técnicas aplicáveis, incluindo procedimentos adequados de manuseio, transporte, recalibração, alinhamento estrutural, configuração eletrônica e testes de desempenho, de modo a preservar a integridade física dos módulos, garantir a continuidade operacional do equipamento e manter os níveis de desempenho e qualidade de imagem originalmente especificados.

Dessa forma, a desinstalação e reinstalação do videowall configuram-se como serviços técnicos indispensáveis, alinhados aos princípios da economicidade, eficiência, razoabilidade e interesse público, evitando a aquisição desnecessária de novos equipamentos e assegurando a adequação da infraestrutura tecnológica às necessidades atuais e futuras da Casa Legislativa.

15. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

A contratação desses serviços garantirá:

1. Aumento da transparência: Permitir que a população e os interessados acompanhem as discussões e decisões tomadas nas reuniões;
2. Maior participação: Incentivar a participação de mais pessoas, incluindo aquelas que
não podem comparecer presencialmente;
3. Melhoria da comunicação: Fornecer uma plataforma para que os membros da equipe e os interessados sejam informados sobre as decisões e ações tomadas;
4. Documentação: Criar um registro permanente das reuniões, permitindo que os interessados revisem e consultem as discussões e decisões a qualquer momento;
5. Aumento da flexibilidade: A transmissão online permite que os interessados participem das reuniões de qualquer lugar e a qualquer hora.
6. Disponibilidade de funcionamento: O suporte e manutenção contínua objetivam manter atualizadas as tecnologias utilizadas na solução própria da Câmara, garantindo a continuidade da prestação desse serviço à sociedade

16. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PARA CONTRATAR

Como solução própria, os servidores já possuem domínio sobre seu funcionamento.

17. INDICAÇÃO DE CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não há

18. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

Não há

19. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO E POSICIONAMENTO CONCLUSIVO SOBRE A CONTRATAÇÃO ADEQUADA À DEMANDA

Estamos considerando a contratação de uma empresa especializada na prestação de Serviços de manutenção preventiva, corretiva e suporte técnico, bem como evolução tecnológica da solução existente dos sistemas de: d

Nesse sentido esta declaração de viabilidade tem como objetivo evidenciar a viabilidade técnica e financeira da contratação desse serviço.

Conclusão

Com base na análise técnica e financeira e operacional, DECLARAMOS que a contratação dessa contratação é viável e recomendada.

14 ÁREA TÉCNICA E SETOR REQUISITANTE

Ricardo Williams Paixão Ferraz
Matrícula - 1016059