



Poder Judiciário

Tribunal de Justiça do Estado do Espírito Santo

Secretaria de Tecnologia da Informação e Comunicação

ESTUDO TÉCNICO PRELIMINAR (ETP) - TIC

Contratação de solução de gestão de identidade, controle de acesso e gerenciamento unificado de dispositivos

SUMÁRIO

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO.....	4
1.1. Contextualização.....	4
1.2. Identificação da demanda no Plano de Contratações de STIC.....	6
2. CARACTERIZAÇÃO DA DEMANDA.....	6
2.1. Descrição da Solução.....	6
2.2. Requisitos necessários e suficientes à escolha da solução de TIC.....	8
2.3. Requisitos Técnicos.....	10
2.4. Requisitos Temporais.....	13
2.5. Requisitos de Segurança da Informação Temporais.....	13
2.6. Requisitos Sociais, Ambientais e Culturais.....	15
2.7. Requisitos Legais.....	16
3. ATENDIMENTO DA DEMANDA.....	16
3.1. Portal de Software Público Brasileiro.....	16
3.1.2. Soluções de TIC.....	16
Solução 1 - Manutenção do ambiente legado (Novell eDirectory + ZENworks).....	16
Solução 2 - Plataforma de identidade de fornecedor independente (IDaaS de terceiros)...	19
Solução 3 - Plataforma de identidade e endpoints em nuvem do ecossistema de produtividade institucional.....	21
3.2. Contratações Públicas Similares.....	26
Órgão 1 - Secretaria de Estado de Planejamento e Gestão de Minas Gerais (SEPLAG/MG).....	26
Órgão 2 - Ministério Público do Estado do Pará (MPPA).....	27
Órgão 3 - Senado Federal.....	27
Órgão 4 - Tribunal de Justiça do Estado da Bahia (TJBA).....	29
Órgão 5 - Agência Nacional de Transportes Aquaviários.....	30
Órgão 6 - Tribunal Regional Federal da 3ª Região.....	31
Órgão 7 - Secretaria de Estado de Planejamento e Gestão de Minas Gerais - SEPLAG/MG.....	32
Órgão 8 - Agência Estadual de Tecnologia da Informação de Pernambuco - ATI/PE.....	33
Órgão 9 - Tribunal de Contas do Estado do Rio Grande do Sul - TCE/RS.....	34
Órgão 10 - Tribunal de Contas do Estado do Rio Grande do Norte - TCE/RN.....	35
3.3. Orçamento Estimado.....	36
5. SUSTENTAÇÃO DO CONTRATO.....	49
5.1. Adequação do Ambiente.....	49
6. ESTRATÉGIA PARA A CONTRATAÇÃO.....	52
6.1. Natureza do Objeto.....	52
6.2. Parcelamento do Objeto e Adjudicação.....	53
6.3. Subcontratação.....	53
6.4. Do Consórcio.....	53



6.5. Modalidade e Tipo da Licitação.....	53
6.6. Vigência do Contrato.....	53
6.7. Equipe de Apoio à Contratação.....	54
7. Equipe de Gestão do Contrato.....	54
8. ANÁLISE DE RISCOS.....	54
8.1. Riscos Mapeados.....	54
APROVAÇÃO E ASSINATURA.....	61
CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC.....	61

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

O Tribunal de Justiça do Estado do Espírito Santo utiliza, como infraestrutura central de autenticação, gestão de identidades e gerenciamento de estações de trabalho, o serviço de diretório Novell eDirectory associado ao Novell ZENworks. Trata-se de plataforma concebida originalmente em 1993, sob a denominação Novell Directory Services, para ambientes corporativos baseados em NetWare, tendo se consolidado, à época, como solução relevante para autenticação centralizada e administração de contas em redes locais. Contudo, a evolução recente do produto foi marcada por sucessivas alterações societárias, com aquisição da Novell pela Attachmate em 2011, posterior incorporação ao portfólio da Micro Focus em 2014 e transferência ao controle da OpenText Corporation em 2023. Esse contexto indica redução progressiva da centralidade estratégica da solução no mercado de tecnologia da informação, com reflexos na disponibilidade de suporte especializado, na amplitude do ecossistema de profissionais certificados e na aderência da plataforma às arquiteturas contemporâneas de identidade, segurança e gerenciamento de dispositivos.

A defasagem tecnológica do ambiente atual produz efeitos operacionais concretos, agravados pela cobertura parcial da solução no TJES. A gestão centralizada de identidades encontra-se implantada apenas no 2º Grau de Jurisdição, ao passo que as Comarcas de 1º Grau distribuídas pelo Estado operam sem acesso unificado, com autenticação local e desarticulada do diretório central. O serviço legado não disponibiliza, de forma nativa, autenticação multifator, acesso condicional, federação por protocolos modernos, como SAML 2.0, OAuth 2.0 e OpenID Connect, nem gerenciamento unificado de dispositivos, capacidades atualmente essenciais para arquiteturas seguras de controle de acessos. Nas Comarcas de 1º Grau, a aplicação de políticas pelo ZENworks vincula-se à relação entre o objeto de usuário e a estação de trabalho, e não propriamente à identidade funcional do colaborador, ocasionando falhas de autenticação na alternância entre equipamentos, perda de mapeamentos de rede e impressoras, além de perfis de usuário que não acompanham servidores e magistrados quando estes transitam entre unidades ou postos de trabalho.

Também se verifica fragilidade no ciclo de vida dos acessos. O remanejamento de lotação depende de processo apenas parcialmente automatizado, em que a retirada dos acessos vinculados ao setor de origem é executada manualmente e sujeita a inconsistências, com

risco de permanência indevida de privilégios após alteração funcional. Esse quadro gera volume recorrente de chamados no Service Desk, consumo de horas técnicas especializadas em atividades repetitivas e aumento da exposição institucional a riscos de segurança da informação, com impacto mais acentuado sobre o 1º Grau, justamente o segmento de maior capilaridade territorial e maior número de unidades administrativas e jurisdicionais do Tribunal.

A contratação também se justifica pela necessidade de adequação do ambiente aos normativos de segurança cibernética, gestão de identidade e proteção de dados aplicáveis ao Poder Judiciário. A manutenção de infraestrutura de identidade sem autenticação multifator nativa, sem suporte adequado a protocolos modernos de federação, sem mecanismos integrados de acesso condicional e sem trilhas de auditoria centralizadas e passíveis de retenção dificulta a plena aderência às diretrizes do Conselho Nacional de Justiça, em especial à Estratégia Nacional de Segurança Cibernética do Poder Judiciário, instituída pela Resolução CNJ nº 396/2021, ao Manual de Referência de Gestão de Identidade e Controle de Acessos, aprovado pela Portaria CNJ nº 162/2021, à obrigatoriedade de autenticação multifator prevista na Portaria CNJ nº 140/2024, aos requisitos de gestão de identidade e controle de acesso da Portaria CNJ nº 408/2024 e aos padrões mínimos de tecnologia da informação fixados pelo Provimento CNJ nº 213/2026. Acresce-se, ainda, o dever de proteção de dados pessoais imposto pela Lei nº 13.709/2018 e pela Resolução CNJ nº 363/2021, que exigem controles de acesso proporcionais, rastreáveis, revisáveis e compatíveis com a criticidade das informações sob a guarda do Tribunal.

Nesse contexto, a solução pretendida consiste na contratação de serviço de controle de acessos fundado em plataforma moderna de gestão de identidade e acesso, integrada a recursos de gerenciamento unificado de dispositivos, apta a prover autenticação multifator, acesso condicional, governança do ciclo de vida das identidades, integração com aplicações institucionais, gerenciamento centralizado de endpoints e auditoria dos acessos. A medida visa substituir gradualmente a dependência do ambiente legado, ampliar a cobertura de identidade para o 1º Grau, reduzir falhas operacionais recorrentes e fortalecer a conformidade do TJES com os normativos do Poder Judiciário, em consonância com a modernização tecnológica conduzida pelo Programa de Modernização do Poder Judiciário do Espírito Santo, financiado pelo Banco Interamericano de Desenvolvimento por meio do Contrato de Empréstimo nº 5883/OC-BR.

1.2. Identificação da demanda no Plano de Contratações de STIC

A presente demanda não consta do Plano de Contratações da Secretaria de Tecnologia da Informação e Comunicação porque sua origem está vinculada ao Programa de Modernização do Poder Judiciário do Estado do Espírito Santo (PROMOJUES), cuja execução possui planejamento próprio, governança específica e financiamento pelo Banco Interamericano de Desenvolvimento (BID), por meio do Contrato de Empréstimo nº 5883/OC-BR.

Embora a solução seja tecnicamente demandada e validada pela área de tecnologia da informação, sua inserção formal no planejamento institucional ocorre no Plano de Aquisições do PROMOJUES, sob o nº **BR-L1620-P00044**, correspondente à contratação **02.03.04.05 - Serviço de Controle de Acessos**. Trata-se, portanto, de contratação de TIC executada no contexto programático do PROMOJUES, com recursos vinculados ao financiamento internacional e submetida ao respectivo sistema de governança, acompanhamento e controle.

A STIC atua como unidade técnica responsável pela definição da necessidade, dos requisitos e da validação da solução.

2. CARACTERIZAÇÃO DA DEMANDA

2.1. Descrição da Solução

A solução pretendida consiste na contratação de serviço de controle de acessos, gestão de identidades e gerenciamento unificado de dispositivos, com vistas à modernização da infraestrutura atualmente utilizada pelo TJES para autenticação de usuários, concessão de permissões, aplicação de políticas de segurança, rastreabilidade de acessos e administração de estações de trabalho.

A solução deverá permitir a centralização do ciclo de vida das identidades digitais de magistrados, servidores, colaboradores, estagiários, terceirizados e demais usuários autorizados, contemplando, no mínimo, os processos de criação, alteração, suspensão, revogação, revisão e auditoria de acessos. Deverá, ainda, viabilizar a aplicação de políticas de acesso baseadas na identidade do usuário, no perfil funcional, na unidade de lotação, no tipo de dispositivo utilizado, no local de acesso e em outros critérios técnicos compatíveis com boas práticas de segurança da informação.

O serviço deverá contemplar mecanismos modernos de autenticação e autorização, incluindo autenticação multifator, acesso condicional, integração com aplicações

institucionais, suporte a padrões abertos de federação de identidade e geração de registros de auditoria suficientes para permitir a rastreabilidade das operações realizadas. Esses recursos são necessários para reduzir a dependência de autenticações locais, ampliar a segurança dos acessos remotos e presenciais e conferir maior controle sobre os privilégios concedidos aos usuários do ambiente tecnológico do TJES.

A solução também deverá abranger recursos de gerenciamento unificado de dispositivos, de forma a permitir o controle centralizado de estações de trabalho, notebooks, dispositivos móveis e demais endpoints institucionais, incluindo inventário, aplicação de políticas, verificação de conformidade, distribuição de configurações, proteção de dados corporativos e integração com os mecanismos de controle de acesso. Essa integração entre identidade e dispositivo é necessária para que o acesso aos sistemas e recursos institucionais considere não apenas a credencial do usuário, mas também a condição de segurança do equipamento utilizado.

Além da substituição gradual das funcionalidades hoje desempenhadas pelo Novell eDirectory e pelo ZENworks, a solução deverá permitir a ampliação do controle centralizado de acessos para as unidades de 1º Grau, que atualmente operam com limitações de integração ao diretório central. Essa ampliação busca reduzir falhas de autenticação, eliminar inconsistências na aplicação de permissões, diminuir chamados recorrentes ao Service Desk e assegurar que o perfil do usuário acompanhe sua movimentação funcional entre unidades, setores e postos de trabalho.

A contratação deverá compreender licenças, subscrições ou direitos de uso necessários à operação da plataforma, bem como os serviços correlatos indispensáveis à sua disponibilização, ativação, configuração inicial, suporte, atualização e manutenção durante a vigência contratual. A solução deverá ser compatível com ambiente corporativo de grande porte, com operação distribuída, alta criticidade, integração com sistemas institucionais e aderência aos normativos de segurança cibernética, proteção de dados pessoais e governança de tecnologia da informação aplicáveis ao Poder Judiciário.

Para fins de planejamento da contratação, considera-se a necessidade de atendimento a aproximadamente 9.000 usuários, distribuídos entre licenças destinadas à camada principal de controle de acessos, identidade e gerenciamento de dispositivos, e licenças com funcionalidades adicionais de produtividade, correio eletrônico, aplicativos corporativos de escritório, armazenamento e colaboração, de modo a contemplar perfis

funcionais que demandem, além dos recursos de identidade e segurança, o uso integrado de ferramentas corporativas de comunicação e trabalho colaborativo.

A composição estimada dos itens a serem contratados é a seguinte:

Item	Descrição	Quantidade
1	Licença ou subscrição para serviço de controle de acessos, gestão de identidades e gerenciamento unificado de dispositivos, contemplando recursos de autenticação multifator, acesso condicional, gerenciamento de identidades, integração com aplicações institucionais, gerenciamento de endpoints e aplicação centralizada de políticas de segurança.	8.500
2	Licença ou subscrição com funcionalidades integradas de controle de acessos, gestão de identidades, aplicativos corporativos de escritório, produtividade, correio eletrônico, armazenamento, colaboração e recursos adicionais de segurança, destinada aos perfis funcionais que demandem, além da camada de identidade e gerenciamento de dispositivos, o uso de ferramentas corporativas para edição de documentos, planilhas, apresentações, comunicação institucional e trabalho colaborativo.	500
3	Serviço técnico especializado, prestado sob demanda, para desenvolvimento, implementação e sustentação das soluções associadas à plataforma de controle de acessos, identidade e gerenciamento de dispositivos, mensurado por hora técnica	2.000

2.2. Requisitos necessários e suficientes à escolha da solução de TIC

A solução de TIC a ser contratada deverá atender a requisitos mínimos de identidade, controle de acesso, gerenciamento de dispositivos, segurança, integração e conformidade normativa, suficientes para substituir gradualmente as funcionalidades atualmente desempenhadas pelo ambiente legado e ampliar o controle centralizado de acessos para o 1º e o 2º Grau de Jurisdição.

Os requisitos foram definidos em nível funcional, de modo a orientar a escolha da solução sem impor especificações excessivas nesta etapa do planejamento, preservando a

análise comparativa das alternativas tecnológicas e do modelo de contratação nos itens próprios deste Estudo Técnico Preliminar.

Nesse contexto, a solução deverá contemplar, no mínimo:

- I. **Gestão de identidades**, permitindo a administração centralizada do ciclo de vida das identidades digitais, incluindo criação, alteração, suspensão, revogação, revisão e auditoria de acessos;
- II. **Controle de acesso** baseado em identidade, permitindo a concessão de permissões com base no usuário, perfil funcional, unidade de lotação, grupos, funções desempenhadas e demais atributos relevantes;
- III. **Autenticação multifator**, possibilitando a adoção de fator adicional de autenticação para acesso a sistemas, aplicações e recursos institucionais, conforme a criticidade do ambiente;
- IV. **Federação e integração de identidade**, com suporte a padrões modernos de autenticação e federação, permitindo integração com sistemas institucionais, aplicações em nuvem e serviços corporativos utilizados pelo PJES;
- V. **Gerenciamento unificado de dispositivos**, abrangendo estações de trabalho, notebooks, dispositivos móveis e demais endpoints institucionais, com recursos de inventário, aplicação de políticas e verificação de conformidade;
- VI. **Segurança da informação**, com controles compatíveis com boas práticas de mercado, incluindo segregação de funções, controle de privilégios, criptografia, logs de segurança e proteção contra acessos não autorizados;
- VII. **Proteção de dados pessoais**, permitindo controles de acesso proporcionais, rastreáveis e revisáveis sobre dados pessoais tratados nos sistemas e serviços do Tribunal;
- VIII. **Continuidade e disponibilidade**, com mecanismos compatíveis com a criticidade dos serviços de identidade e controle de acesso, reduzindo risco de indisponibilidade dos sistemas institucionais;
- IX. **Migração e transição gradual**, admitindo coexistência temporária com o ambiente legado e transição controlada das identidades, dispositivos, políticas e integrações;
- X. **Suporte técnico e atualização**, contemplando suporte, atualizações, correções de segurança e manutenção durante a vigência contratual;
- XI. **Modelo de licenciamento compatível**, considerando os quantitativos estimados e a existência de perfis funcionais distintos, inclusive usuários que demandem recursos

adicionais de produtividade, correio eletrônico, aplicativos corporativos de escritório e colaboração;

Os requisitos acima constituem o conjunto mínimo necessário à caracterização da solução de TIC pretendida, sem prejuízo de detalhamento posterior no Termo de Referência, especialmente quanto às especificações técnicas, níveis de serviço, obrigações da CONTRATADA, forma de implantação, critérios de aceite, suporte, segurança e gestão contratual.

2.3. Requisitos Técnicos

2.3.1. A solução deverá atender, no mínimo, aos requisitos técnicos especificados nesta seção, segmentados conforme os dois tipos de licença que compõem a contratação, observados os perfis de uso institucional e os padrões abertos de mercado.

2.3.2. Licença de Controle de Acessos, Identidade e Gerenciamento de Dispositivos

2.3.2.1. Licença destinada à camada de identidade, controle de acessos e gerenciamento de dispositivos, aplicável à totalidade dos usuários institucionais, fornecida em modelo de serviço gerenciado em nuvem, devendo atender, no mínimo, aos seguintes requisitos:

- I. Diretório de identidades em nuvem, com administração centralizada do ciclo de vida das identidades digitais, incluindo criação, alteração, suspensão, revogação, revisão periódica e auditoria de contas e acessos.
- II. Autenticação única (Single Sign-On) para aplicações internas e em nuvem, com suporte nativo aos protocolos SAML 2.0, OAuth 2.0 e OpenID Connect, e provisionamento de contas por meio de SCIM.
- III. Autenticação multifator com suporte a, no mínimo, aplicativo autenticador, chave de segurança no padrão FIDO2, senha de uso único e notificação por dispositivo.

- IV. Acesso condicional por políticas, com avaliação de usuário, grupo, perfil funcional, dispositivo, localização, estado de conformidade e nível de risco da sessão.
- V. Governança de identidade, com provisionamento e desprovisionamento automatizados, revisão periódica de acessos, controle de grupos e fluxos de aprovação.
- VI. Gestão de acesso privilegiado, com elevação de permissões controlada e temporária e registro das ações executadas.
- VII. Gerenciamento unificado de dispositivos, abrangendo estações de trabalho, notebooks e dispositivos móveis, com inventário, aplicação remota de políticas, verificação de conformidade, distribuição de configurações e proteção de dados corporativos no dispositivo.
- VIII. Integração entre identidade e dispositivo, condicionando a concessão de acesso à credencial do usuário e ao estado de segurança e conformidade do equipamento.
- IX. Trilhas de auditoria íntegras dos eventos de autenticação, autorização e administração, com retenção e suporte a integração com plataforma de correlação de eventos de segurança (SIEM).
- X. Criptografia dos dados em trânsito por TLS 1.2 ou superior e em repouso em padrão equivalente a AES-256 ou superior.

2.3.3. Licença de Controle de Acessos com Recursos de Produtividade e Colaboração

- 2.3.3.1. Licença destinada ao subconjunto de usuários que demandem, além da camada de identidade e gerenciamento de dispositivos, ferramentas corporativas de produtividade e comunicação, integrada à mesma base de identidade e sem

duplicação de credenciais, devendo atender, no mínimo, aos seguintes requisitos:

- I. Integralidade dos requisitos previstos no item anterior, sobre a mesma base de diretório.
- II. Aplicativos corporativos de produtividade para edição de documentos de texto, planilhas e apresentações, nas modalidades instalável e web.
- III. Correio eletrônico corporativo com caixa postal individual de capacidade compatível com o uso institucional, calendário e contatos integrados.
- IV. Armazenamento individual em nuvem, com recursos de colaboração e compartilhamento de arquivos sob controle de permissões.
- V. Plataforma de comunicação e colaboração corporativa, com mensageria, reuniões e trabalho em equipe, integrada à identidade institucional.
- VI. Aplicação das mesmas políticas de autenticação multifator, acesso condicional, auditoria e proteção de dados exigidas para a camada de identidade.

2.3.4. Serviços Técnicos Especializados em Desenvolvimento, Implementação e Sustentação

2.3.4.1. Serviço técnico especializado, destinado ao desenvolvimento, à implementação e à sustentação das soluções associadas à plataforma contratada, mensurado por hora técnica, com o objetivo de assegurar a operação, a evolução e a continuidade do ambiente durante toda a vigência contratual, devendo contemplar, no mínimo:

- I. Desenvolvimento, customização e sustentação de soluções sobre a plataforma, incluindo painéis, aplicações, fluxos automatizados, agentes e serviços

em nuvem, bem como o suporte a soluções instaladas no ambiente da contratante.

- II. Avaliação e otimização do ambiente, migração de sistemas, integração de soluções e implementação de novos serviços, conforme a demanda institucional.
- III. Definição de políticas operacionais, elaboração de scripts e atividades de monitoramento, com execução de intervenções preventivas e corretivas voltadas ao desempenho e à segurança do ambiente.
- IV. Prestação do serviço em regime de disponibilidade compatível com a criticidade das atividades suportadas, observada a natureza da demanda.

2.4. Requisitos Temporais

- 2.4.1. As licenças de subscrição deverão ser disponibilizadas em até 10 (dez) dias úteis, contados da assinatura do contrato.
- 2.4.2. O prazo de disponibilização das licenças poderá ser prorrogado por igual período, mediante justificativa formal aceita pelo CONTRATANTE.
- 2.4.3. A disponibilização das licenças será comprovada mediante ativação efetiva no ambiente da contratante, apta ao uso pelos usuários institucionais.
- 2.4.4. Os serviços técnicos especializados terão reunião inicial em até 2 (dois) dias úteis e início da execução em até 5 (cinco) dias úteis após a reunião inicial, contados da solicitação do CONTRATANTE.

2.5. Requisitos de Segurança da Informação Temporais

- 2.5.1. São requisitos exigidos com relação à Política de Segurança da Informação, na forma da Resolução nº 079/2024, do Ato Normativo nº 41/2018 e do Ato Normativo nº 42/2018, do Ato Normativo nº 161/2024, do Ato Normativo nº 124/2024, do Ato Normativo nº 143/2024, Ato normativo nº 240/2024, Ato normativo nº 139/2024, Ato normativo nº 145/2024 todos deste PJES, devendo a CONTRATADA:
 - 2.5.1.1. Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo CONTRATANTE.

- 2.5.1.2. Executar todos os testes de segurança necessários e definidos nas legislações pertinentes, bem como executar seus trabalhos dentro das diretrizes ali estabelecidas.
- 2.5.1.3. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do PJES ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar seus empregados nesse sentido.
- 2.5.1.4. Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos eventualmente disponibilizados para a execução dos serviços, não cabendo ao PJES qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer, cabendo à CONTRATADA o seu ressarcimento, em quantidade e qualidade, sem prejuízo das penalidades cabíveis.
- 2.5.1.5. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do PJES.
- 2.5.1.6. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou de rescisão do Contrato, as informações relativas:
 - 2.5.1.6.1. À Política de Segurança adotada pelo PJES e as configurações de hardware e de softwares decorrentes;
 - 2.5.1.6.2. Ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos;
 - 2.5.1.6.3. Ao processo de implementação, no ambiente do PJES, dos mecanismos de criptografia e autenticação.
- 2.5.1.7. A Lei Geral de Proteção de Dados será obedecida, em todos os seus termos, pela CONTRATADA, obrigando-se ela a tratar os dados da CONTRATANTE que forem eventualmente coletados, conforme sua necessidade ou obrigatoriedade. (art. 7º, LGPD).
- 2.5.1.8. Conforme prevê a Lei Geral de Proteção de Dados, obriga-se a CONTRATADA a executar os seus trabalhos e tratar os dados da CONTRATANTE respeitando os princípios da

finalidade, adequação, transparência, livre acesso, segurança, prevenção e não discriminação (art. 6º, LGPD).

2.6. Requisitos Sociais, Ambientais e Culturais

- 2.6.1. A CONTRATADA deverá orientar sua equipe técnica sobre as boas práticas voltadas ao consumo consciente, redução de desperdício dos recursos naturais e coleta seletiva, inclusive à adequada destinação dos resíduos porventura gerados na execução do contrato, com o objetivo de contribuir para a preservação do meio ambiente, quando aplicável;
- 2.6.2. Os profissionais da CONTRATADA que desempenharão as atividades em contato direto junto ao CONTRATANTE, deverão cumprir os seguintes requisitos:
 - 2.6.2.1. Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando vestuário que comprometa a imagem institucional do CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;
 - 2.6.2.2. Respeitar todos os servidores e demais colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;
 - 2.6.2.3. Atuar nas dependências do CONTRATANTE, se necessário, com urbanidade e cortesia.
- 2.6.3. Quanto aos critérios ambientais, a CONTRATADA deverá cumprir os seguintes requisitos de uso racional de recursos:
 - 2.6.3.1. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);
 - 2.6.3.2. As configurações de hardware e software deverão ser realizadas visando ao alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;
 - 2.6.3.3. Utilizar de forma eficiente o espaço de armazenamento virtual e oferecer o máximo de desempenho de processamento com o menor impacto ou comprometimento

da capacidade de processamento dos recursos tecnológicos do CONTRATANTE.

2.7. Requisitos Legais

- 2.7.1. A pretensa contratação tem como referência os seguintes instrumentos legais: Constituição Federal de 1988; Lei nº 14.133/2021; Resolução nº 468/2022 do CNJ; Instrução Normativa nº 94/2022 do ME; e demais instrumentos correlatos.

3. ATENDIMENTO DA DEMANDA

3.1. Portal de Software Público Brasileiro

- 3.1.1. Foi realizada consulta ao Portal do Software Público Brasileiro, não tendo sido identificada solução de gestão de identidade e controle de acessos com gerenciamento unificado de dispositivos capaz de atender, de forma nativa e auditável, aos requisitos de segurança da informação exigidos pelos normativos do CNJ, em especial a autenticação multifator, o acesso condicional e a governança automatizada do ciclo de vida das identidades. Não há, portanto, alternativa de software público apta a suprir a demanda.

3.1.2. Soluções de TIC

- 3.1.2.1. A análise comparativa considerou, além do aspecto econômico, os aspectos qualitativos relativos ao atendimento dos objetivos da contratação e à conformidade normativa, observando as soluções adotadas por outros órgãos da Administração Pública para necessidades similares.

Solução 1 - Manutenção do ambiente legado (Novell eDirectory + ZENworks)

Esta alternativa consiste em preservar o serviço de diretório Novell eDirectory e a ferramenta ZENworks em operação no Tribunal, eventualmente acrescidos dos produtos complementares da mesma família corporativa (Identity Manager, Access Manager, Advanced Authentication) para suprir as ausências de autenticação moderna e gerenciamento de dispositivos, mantendo a arquitetura de identidade assentada em infraestrutura local. A favor dessa opção pesam a dispensa de investimento inicial em migração e o aproveitamento do conhecimento operacional acumulado pela equipe sobre uma plataforma em produção há anos, com rotinas administrativas consolidadas no 2º Grau

de Jurisdição. A continuidade evita a curva de aprendizado de uma nova solução e a disrupção inerente a qualquer transição de serviço de diretório, componente sensível por concentrar a autenticação de todos os sistemas. Em um cenário hipotético de estabilidade tecnológica e ausência de novas exigências regulatórias, a manutenção seria a opção de menor esforço imediato.

Essas vantagens, contudo, não resistem ao exame do ciclo de vida do produto e da sua sustentação no mercado. O eDirectory foi concebido em 1993, sob a denominação Novell Directory Services, para ambientes baseados em NetWare, e ao longo de três transferências sucessivas de titularidade corporativa, Attachmate em 2011, Micro Focus em 2014 e OpenText em 2023, sofreu desinvestimento progressivo em pesquisa e desenvolvimento, sem inovações relevantes desde 2015 e com roadmap restrito à manutenção evolutiva mínima. A consequência direta para o Tribunal é dupla: a dependência de um produto cuja trajetória aponta para a descontinuação e a contração crítica da base de profissionais certificados no mercado brasileiro, que reduz a capacidade de contratar suporte especializado e eleva o risco operacional sobre uma infraestrutura permanente. Para um ativo que concentra a identidade institucional, operar sem garantia de continuidade de longo prazo é risco de difícil mitigação.

A limitação se aprofunda na autenticação. O eDirectory não implementa autenticação multifator de forma nativa em nenhuma de suas versões, nem suporta nativamente os protocolos de federação OAuth 2.0, OpenID Connect e SAML 2.0, que são a base da autenticação contemporânea e da integração com serviços em nuvem e portais governamentais. Esse déficit colide frontalmente com a Portaria CNJ nº 140/2024, que tornou o MFA obrigatório e de eficácia imediata para o acesso a sistemas judiciais sensíveis, sem admitir atendimento parcial ou postergação. Suprir a ausência exigiria sobrepor ao eDirectory produtos de terceiros de autenticação forte e de federação, solução que não elimina a dependência da base legada, multiplica os pontos de falha e onera o ambiente com licenças e contratos de suporte adicionais. No gerenciamento de dispositivos a deficiência se repete, pois o ZENworks não oferece gerenciamento unificado de endpoints para o parque moderno do Tribunal, Windows 11, iOS e Android, no padrão exigido por uma arquitetura de controle de acessos atual, em que a concessão de acesso depende da verificação de conformidade do dispositivo, criptografia de disco, versão de sistema e postura de segurança, antes da liberação. Sem essa capacidade, o controle de acesso fica restrito à credencial do usuário e ignora o estado do equipamento, e a proteção de dados corporativos no dispositivo torna-se inviável de forma centralizada, ao passo que a

integração com o ecossistema de produtividade em nuvem já adotado pela instituição permanece inexistente ou severamente limitada.

Para além de exigências isoladas, a manutenção do ambiente legado configura não atendimento a um conjunto articulado de normas de observância obrigatória. A Resolução CNJ nº 396/2021 (ENSEC-PJ) exige capacidades nativas de prevenção, detecção e resposta a incidentes e a preservação da disponibilidade, integridade, confidencialidade e autenticidade dos ativos. A Portaria CNJ nº 162/2021 impõe gestão centralizada de identidades com segregação de funções, controle de acesso baseado em funções (RBAC), provisionamento e desprovisionamento automatizados vinculados ao ciclo de vida funcional e revisões periódicas de acesso. A Portaria CNJ nº 316/2023 determina contas individuais, intransferíveis e integráveis ao Sistema de Controle de Acessos Corporativo do CNJ por federação. A Portaria CNJ nº 408/2024 acrescenta acesso condicional, detecção de risco e bloqueio automático de contas diante de atividade suspeita. O eDirectory não atende nativamente a esses comandos, e alcançar resultado equivalente exigiria empilhar produtos complementares, cada um com seu ciclo de suporte, custo e superfície de risco, o que aumenta a complexidade e enfraquece justamente a auditabilidade e a rastreabilidade que as normas pretendem assegurar. O mesmo descompasso se observa frente aos referenciais técnicos de mercado, ABNT NBR ISO/IEC 27001:2022 nos controles de acesso e de acesso privilegiado, NIST SP 800-207 na arquitetura Zero Trust, NIST SP 800-53 Rev. 5 nos controles IA-2, AC-2 e AU-2, e CIS Controls v8 nos controles 5 e 6, cujo atendimento pressupõe avaliação contínua e adaptativa de cada solicitação de acesso, modelo estranho à arquitetura do eDirectory. Soma-se a isso a proteção de dados pessoais, pois a Resolução CNJ nº 363/2021 e a Lei nº 13.709/2018 (LGPD) impõem ao Tribunal o controle granular, rastreável e revisável de quem acessa dados pessoais e em que circunstâncias, com responsabilização objetiva do controlador em caso de falha, enquanto o eDirectory oferece apenas logs básicos e integração limitada com plataformas de correlação de eventos (SIEM), o que dificulta a demonstração de conformidade e a resposta tempestiva a incidentes.

O agravante decisivo é territorial. A gestão de identidades está implantada apenas no 2º Grau de Jurisdição, e todas as Comarcas de 1º Grau operam sem acesso unificado, com autenticação local e desarticulada do diretório central. Manter o eDirectory perpetuaria a não conformidade onde ele já opera e deixaria sem solução o 1º Grau, segmento de maior capilaridade territorial e maior número de unidades do Tribunal, pois estender a plataforma legada a todo o Estado, para corrigir a assimetria, significaria investir na expansão de uma

tecnologia em fim de ciclo e incapaz de atender aos requisitos normativos, decisão tecnicamente regressiva. A esse quadro acresce o custo total de propriedade, já que o licenciamento perpétuo com manutenção anual crescente onera o Tribunal por capacidades cada vez mais restritas, e a sobreposição de produtos complementares necessária para aproximar o ambiente legado da conformidade adicionaria novos custos de licença, integração e suporte, resultado desfavorável quando comparado ao modelo de subscrição por usuário, previsível e escalável, sem investimento em servidores locais.

A manutenção do ambiente legado apresenta, em síntese, como única vantagem relevante a menor interrupção imediata, benefício anulado por um conjunto convergente de contras: risco concreto de descontinuidade do produto e do suporte, ausência nativa de autenticação multifator, de federação moderna, de acesso condicional e de governança de identidade, incapacidade de gerenciamento unificado de dispositivos, não atendimento a normas do CNJ de cumprimento obrigatório e aos referenciais técnicos de mercado, fragilidade na proteção de dados pessoais, permanência do 1º Grau desassistido e custo total de propriedade desfavorável. A alternativa não se sustenta como solução viável para a necessidade identificada, servindo de marco comparativo que evidencia a necessidade de substituição.

Solução 2 - Plataforma de identidade de fornecedor independente (IDaaS de terceiros)

Esta alternativa consiste em adotar uma plataforma de identidade como serviço (IDaaS) ofertada por fornecedor não vinculado ao ecossistema de produtividade já utilizado pelo Tribunal, a exemplo de Okta, Ping Identity, OneLogin ou ForgeRock, no modelo de serviço em nuvem. São plataformas especializadas em gestão de identidade e acesso, com posição consolidada no mercado corporativo e maturidade reconhecida na função para a qual foram concebidas.

A favor dessa opção pesa a robustez das capacidades de identidade. As plataformas IDaaS líderes entregam, de forma nativa, diretório de identidades unificado, autenticação única (SSO) sobre os protocolos abertos SAML 2.0, OAuth 2.0 e OpenID Connect, autenticação multifator com múltiplos métodos, acesso condicional baseado em contexto e risco, e governança do ciclo de vida das identidades com provisionamento e desprovisionamento automatizados nos fluxos de admissão, movimentação e desligamento. Algumas oferecem ainda motores de automação sem código para esses fluxos e ampla biblioteca de integrações com aplicações de terceiros, o que as torna particularmente atraentes para organizações que adotam estratégia multifornecedor e desejam justamente evitar a

dependência de um único fabricante. Sob o ângulo estrito da gestão de identidade e do controle de acessos, portanto, a solução atende aos requisitos técnicos definidos neste Estudo e às determinações do CNJ em matéria de autenticação forte, acesso condicional e governança de identidade.

A adequação ao caso concreto do Tribunal, contudo, é prejudicada por duas ordens de limitação. A primeira é a ausência de gerenciamento unificado de dispositivos (UEM/MDM) nativo. As plataformas IDaaS independentes são, em regra, especializadas na camada de identidade e não incorporam gerenciamento de endpoints próprio, de modo que o requisito de verificar a conformidade do dispositivo, criptografia de disco, versão de sistema e postura de segurança, como condição para a concessão de acesso depende da integração com uma solução de UEM de terceiro, contratada e mantida separadamente. Isso fragmenta em dois contratos e dois fornecedores aquilo que a necessidade do Tribunal trata como um único serviço de controle de acessos, com gerenciamento de dispositivos acoplados, ampliando a superfície de integração, os pontos de falha e o custo total.

A segunda limitação é a camada adicional de integração com o ambiente de produtividade já instalado. Como a plataforma IDaaS não pertence ao mesmo ecossistema das ferramentas de produtividade e correio eletrônico utilizadas pela instituição, a federação entre identidade e essas aplicações, embora tecnicamente viável pelos protocolos abertos, exige configuração, conectores e manutenção contínua dessa ponte, sem o ganho de transparência operacional que a aderência nativa ao ecossistema proporcionaria. A literatura técnica e os comparativos de mercado registram, ademais, que a configuração de políticas adaptativas e de acesso condicional nessas plataformas tem curva de aprendizado acentuada e demanda equipe técnica dedicada, com funcionalidades de maior valor frequentemente concentradas nos planos de licenciamento superiores, o que eleva o custo efetivo da solução conforme se ativam os recursos exigidos pelos normativos.

O resultado é uma alternativa tecnicamente capaz na camada de identidade, mas economicamente e operacionalmente menos vantajosa para o Tribunal do que uma solução que entregue identidade e gerenciamento de dispositivos de forma integrada e aderente ao ecossistema já existente. A adoção do IDaaS de terceiro resolveria a questão da autenticação e da governança de identidade, porém ao custo de uma arquitetura mais fragmentada, de maior esforço de integração e de sustentação, e de uma duplicação de fornecedores para compor o mesmo serviço, razões pelas quais não se mostra a opção mais adequada à necessidade identificada, ainda que constitua alternativa viável e seja útil

como termo de comparação que confirma a maturidade do mercado de identidade em nuvem.

Solução 3 - Plataforma de identidade e endpoints em nuvem do ecossistema de produtividade institucional

Esta alternativa consiste na adoção de plataforma de gestão de identidade e acesso (IAM) integrada nativamente a gerenciamento unificado de endpoints (UEM), ofertada no modelo de serviço em nuvem e pertencente ao mesmo ecossistema das ferramentas de produtividade e correio eletrônico já utilizadas pelo Tribunal. A solução reúne em um único serviço, e sobre uma única base de identidade, as duas camadas que a necessidade do Tribunal trata como indissociáveis: o controle de acessos e o gerenciamento dos dispositivos a partir dos quais esses acessos são exercidos.

A plataforma de identidade entrega, de forma nativa, diretório de identidades unificado para usuários, grupos, dispositivos, aplicações e identidades de serviço; autenticação única (SSO) sobre os protocolos abertos SAML 2.0, OAuth 2.0 e OpenID Connect; autenticação multifator com amplo espectro de métodos, incluindo aplicativo autenticador, chaves de segurança FIDO2, senha de uso único e biometria; acesso condicional com políticas granulares avaliadas a partir de usuário, dispositivo, localização, nível de risco e sensibilidade da aplicação; detecção de risco de identidade com análise comportamental, capaz de sinalizar logins suspeitos, credenciais vazadas e deslocamentos geograficamente improváveis; gestão de acesso privilegiado com elevação temporária e controlada de permissões, fluxo de aprovação e auditoria; e governança do ciclo de vida das identidades, com provisionamento e desprovisionamento automatizados, revisões periódicas de acesso e pacotes de acesso. A camada de gerenciamento de dispositivos administra estações Windows e macOS e dispositivos móveis iOS e Android a partir de console único em nuvem, sem servidores locais, aplicando políticas de conformidade, inventário de hardware e software, distribuição de configurações, gerenciamento de criptografia de disco, proteção de dados corporativos no dispositivo e remediação automatizada.

O que distingue tecnicamente esta solução das demais é a operação conjunta dessas duas camadas como arquitetura única de *Zero Trust*. Nenhum usuário ou dispositivo detém confiança implícita, e cada solicitação de acesso é avaliada de forma contínua e adaptativa com base na identidade verificada, na postura de segurança do dispositivo, na localização da conexão e na sensibilidade do recurso. Essa convergência de variáveis em um único mecanismo de acesso condicional elimina a fragmentação de políticas característica de

arquiteturas montadas a partir de produtos distintos, e produz exatamente a coerência, a automação e a auditabilidade que os normativos do CNJ exigem. É essa integração nativa entre identidade e dispositivo que a Solução 2 não oferece sem acoplar um produto de UEM de terceiro, e que o ambiente legado da Solução 1 é estruturalmente incapaz de prover.

A aderência ao ecossistema de produtividade já instalado no Tribunal é o segundo fator decisivo. Por pertencer à mesma família dos sistemas operacionais adotados pelo PJES, a plataforma federa-se a esses sistemas de forma transparente, sem a camada adicional de conectores e manutenção contínua que uma solução de fornecedor independente exigiria, e preserva uma única identidade institucional para o usuário em todos os serviços. A integração híbrida com o diretório local eventualmente mantido é suportada nativamente, o que viabiliza uma transição gradual a partir do ambiente atual, e a interoperabilidade com os sistemas judiciais e administrativos, incluindo PJe e SEI, é assegurada pelos protocolos abertos de federação. Essa aderência reduz o esforço de integração, encurta a curva de aprendizado da equipe técnica e diminui o custo total de propriedade, ao dispensar a contratação e a sustentação de produtos avulsos para compor o mesmo serviço.

A conformidade normativa é o terceiro fator, e é integral. A solução atende nativamente à obrigatoriedade de autenticação multifator da Portaria CNJ nº 140/2024, aos requisitos de gestão centralizada de identidades, RBAC, provisionamento automatizado e revisão de acessos da Portaria CNJ nº 162/2021, à exigência de contas individuais e federáveis ao Sistema de Controle de Acessos Corporativo da Portaria CNJ nº 316/2023, e aos comandos de acesso condicional, detecção de risco e bloqueio automático de contas da Portaria CNJ nº 408/2024, tudo em linha com os objetivos da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (Resolução CNJ nº 396/2021). No tocante à proteção de dados pessoais, oferece controle granular de permissões, trilha de auditoria completa com identificação de usuário, recurso, horário e localização, integração nativa com plataforma de correlação de eventos (SIEM) e criptografia em trânsito e em repouso, com certificações independentes de segurança da informação, atendendo aos deveres impostos pela Resolução CNJ nº 363/2021 e pela Lei nº 13.709/2018 (LGPD). O alinhamento se estende aos referenciais técnicos de mercado, ABNT NBR ISO/IEC 27001:2022, NIST SP 800-207, NIST SP 800-53 Rev. 5 e CIS Controls v8, cujos controles de acesso, identidade e auditoria são atendidos nativamente.

A materialização dessa solução dá-se por meio da adesão à Ata de Registro de Preços decorrente do Pregão Eletrônico para Registro de Preços nº 082/2025 da Secretaria de

Estado de Planejamento e Gestão de Minas Gerais (SEPLAG/MG), homologado em 29 de agosto de 2025, cujo objeto é a aquisição de licenças no modelo de subscrição, com previsão expressa de adesão por órgãos não participantes. Dentro desta ata, a solução é composta por dois itens que correspondem, com precisão técnica, aos dois tipos de licença especificados no item 2.3 deste Estudo. O item com SKU AAA-10732 do Detalhamento do Objeto, relativo à licença Enterprise Mobility + Security E3 (EMS E3), incorpora o serviço de diretório de identidades em nuvem com gerenciamento de acesso de nível Premium e a solução de gerenciamento unificado de dispositivos, sendo tecnicamente equivalente à Licença de Controle de Acessos, Identidade e Gerenciamento de Dispositivos descrita no item 2.3.2, razão pela qual atende ao perfil da totalidade dos usuários e responde pelo quantitativo de 8.500 licenças. O item com SKU AAD-33204 do Detalhamento do Objeto, relativo à licença Microsoft 365 E3, incorpora a mesma camada de identidade e gerenciamento de dispositivos e acrescenta a ela a suíte de produtividade, o correio eletrônico e os recursos de colaboração, sendo tecnicamente equivalente à Licença de Controle de Acessos com Recursos de Produtividade e Colaboração descrita no item 2.3.3, destinando-se ao subconjunto de 500 usuários que demandem também a produtividade integrada.

A equivalência entre os dois itens merece registro, porque é ela que assegura a coerência arquitetural da solução. Tanto o item com SKU AAA-10732 quanto o item com SKU AAD-33204 assentam-se sobre a mesma base de identidade e sobre o mesmo serviço de gerenciamento de dispositivos, diferindo apenas pela presença, no item com SKU AAD-33204, da camada de produtividade e correio. Em consequência, a totalidade dos 9.000 usuários opera sob uma única plataforma de controle de acessos, com as mesmas políticas de autenticação multifator, acesso condicional, auditoria e proteção de dados aplicadas de modo uniforme, sem fragmentação da identidade e sem coexistência de mecanismos de autenticação distintos entre os perfis. Essa unicidade de base é precisamente o que o item 2.3.3.1 deste Estudo exige ao determinar que a licença com produtividade contemple a integralidade dos requisitos de identidade e dispositivos do item 2.3.2 sobre a mesma base de diretório.

A escolha pela solução do ecossistema Microsoft, em detrimento das plataformas de identidade de fornecedores independentes analisadas na Solução 2, não decorre de preferência pela marca, mas de fatos objetivos do ambiente do Tribunal. O parque computacional da instituição opera majoritariamente sobre o ecossistema Microsoft, com sistema operacional dessa origem nas estações de trabalho e ferramentas de produtividade

já utilizadas em grande parte das unidades. A adoção de uma plataforma de identidade e gerenciamento de dispositivos pertencente a esse mesmo ecossistema federa-se de forma nativa ao ambiente existente, sem a camada de conectores e de manutenção contínua que uma solução de terceiro exigiria para se comunicar com as aplicações de produtividade e com os endpoints já em uso. Essa aderência produz três ganhos concretos: a integração transparente entre identidade, dispositivos e produtividade sobre uma base única, sem fragmentação; a substancial facilidade na transição, uma vez que o gerenciamento dos dispositivos Windows já existentes e a sincronização com o diretório atual são suportados nativamente, permitindo migração gradual e de menor risco; e a redução do esforço de sustentação e da curva de aprendizado da equipe técnica, que passa a administrar identidade e dispositivos no mesmo ecossistema com que já opera. As plataformas independentes, embora tecnicamente capazes na camada de identidade, imporiam ao Tribunal a integração de produtos distintos e a manutenção de pontes entre fornecedores para alcançar resultado que a solução aderente entrega de forma nativa, o que a torna a opção tecnicamente mais adequada ao caso concreto, na mesma lógica de padronização e interoperabilidade que ampara a exigência de marca no instrumento de origem a que se pretende aderir.

A esses fatores soma-se a sustentação de mercado. Diferentemente do produto legado, trata-se de plataforma estratégica para o fornecedor, com evolução contínua, e que conta com o maior ecossistema de parceiros e de profissionais qualificados disponível no mercado brasileiro, o que reduz o risco operacional e de descontinuidade sobre uma infraestrutura de natureza crítica e permanente. O modelo de licenciamento por subscrição por usuário, mensal e escalável, confere previsibilidade orçamentária e dispensa investimento em servidores locais.

Por reunir, em um único serviço aderente ao ambiente já existente, o controle de acessos e o gerenciamento de dispositivos exigidos, por atender integralmente e de forma nativa às normas do CNJ e aos referenciais técnicos aplicáveis, por corresponder com exatidão aos requisitos técnicos especificados no item 2.3 por meio dos itens com SKU AAA-10732 e AAD-33204 da ata da SEPLAG/MG, por aderir ao parque computacional majoritariamente padronizado no ecossistema Microsoft e viabilizar transição de menor risco, e por resolver a assimetria entre 1º e 2º Graus com a extensão da gestão unificada de identidades a todas as Comarcas, esta é a solução escolhida. A demonstração da vantajosidade técnica e econômica da escolha, inclusive frente a contratações públicas similares dos últimos cinco



Poder Judiciário

Tribunal de Justiça do Estado do Espírito Santo

Secretaria de Tecnologia da Informação e Comunicação

anos, e a respectiva estimativa de custo são desenvolvidas nos itens subsequentes deste Estudo.



3.2. Contratações Públicas Similares

3.2.1. Foram identificadas contratações públicas similares no âmbito do Poder Judiciário e da Administração Pública, comprovando a maturidade, a viabilidade e a adequação da solução de identidade e endpoints em nuvem para o contexto institucional, conforme detalhado abaixo:

Órgão 1 - Secretaria de Estado de Planejamento e Gestão de Minas Gerais (SEPLAG/MG)

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAA-10732	AAD-33204	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO
Aquisição de licenças de software no modelo de subscrição (controle de acessos, identidade e gerenciamento de dispositivos) ¹	Pregão Eletrônico SRP nº 0000000082/2025 (Proc. nº 1500.01.0595970/2024-80)	Homologa do em 29/08/2025	Brasoftware Informática Ltda. (CNPJ 57.142.978/0001-05)	Quantidade 28.895	Quantidade 34.950	Quantidade/Horas 131.620	R\$ 25.831.113,35
				Valor Unit. Mensal R\$ 42,63	Valor Unit. Mensal R\$ 176,61	Valor Unitário R\$ 140,00	

¹ Observação: o valor informado refere-se exclusivamente aos itens objeto da pretendida adesão, a saber, a licença EMS E3 - AAA-10732 (8.500 licenças, ao valor unitário mensal de R\$ 42,63) e a licença Microsoft 365 E3 - AAD-33204 (500 licenças, ao valor unitário mensal de R\$ 176,61), homologadas em favor da empresa Brasoftware Informática Ltda., calculado para o período de 12 (doze) meses. Não corresponde ao valor total da Ata de Registro de Preços, que abrange dezenas de outros itens estranhos a esta contratação, restrição adotada para preservar a pertinência e a clareza da avaliação comparativa.



Órgão 2 - Ministério Público do Estado do Pará (MPPA)

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAA-10732	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO
Registro de Preços para a prestação de serviços do fabricante Microsoft, incluindo subscrição de licenças de uso de software, serviços de computação em nuvem e serviços técnicos especializados, decorreu de Licitação na modalidade Pregão Eletrônico ¹	1º Termo Aditivo à Ata de Registro de Preços nº 015/2024-MPPA, decorrente do Pregão Eletrônico nº 021/2024-MPPA, Protocolo GEDOC nº 150572/2025	Vigência prorrogada por 12 meses, de 11/09/2025 a 10/09/2026	Lanlink Soluções e Comercialização em Informática S/A, CNPJ 19.877.285/0001-71	Quantidade 1.818	Quantidade/Horas 2.500	R\$ 3.973.574,22
				Valor Unit. Mensal R\$ 1.991,79	Valor Unitário R\$ 141,00	

¹ Observação: o valor informado refere-se exclusivamente ao item 8 do 1º Termo Aditivo à ARP nº 015/2024-MPPA, correspondente ao SKU AAA-10732, EMS E3, com quantidade de 1.818 licenças, preço unitário de R\$ 1.991,79 e valor global do item de R\$ 3.973.574,22. Não corresponde ao valor total da Ata de Registro de Preços, que contempla diversos outros itens e serviços Microsoft.

Órgão 3 - Senado Federal

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAA-10732	PREÇO TOTAL DO CONTRATO
---------	------------------------------	-------------	-------------------	-----------	-------------------------



Fornecimento de licenças de uso por tempo indeterminado e subscrição de software Microsoft, na modalidade Enterprise Agreement para equipamentos servidores do Senado Federal, bem como prestação de serviços de subscrição ou licenças de uso para ferramentas de colaboração, correio eletrônico, armazenamento, produtividade e IA generativa, pelo período de 36 (trinta e seis) meses.	Contrato nº 12/2025, Pregão Eletrônico nº 900002/2025, Processo nº 200017489202488	Assinatura em 22/01/2025, vigência de 22/01/2025 a 22/01/2028	Brasoftware Informática Ltda., CNPJ 57.142.978/0001-05	Quantidade 7.029	R\$ 12.156.233,76
				Valor Unit. Mensal R\$ 48,04	

¹ Observação: o valor informado refere-se exclusivamente ao item 13 do Contrato nº 012/2025, correspondente ao SKU AAA-10732, EMS E3, com quantidade de 7.029 licenças, preço unitário de R\$ 1.729,44 e valor global do item de R\$ 12.156.233,76. Não corresponde ao valor total do contrato, que contempla diversos outros itens e serviços Microsoft.



Órgão 4 - Tribunal de Justiça do Estado da Bahia (TJBA)

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAA-10732	PREÇO TOTAL DO CONTRATO (36 meses)
Contratação de subscrições Microsoft e renovação de licenças (Software Assurance), além de prestação de Serviço Gerenciado e Suporte Continuo na plataforma Microsoft Office 365, em conformidade com as condições, quantidades e exigências estabelecidas neste instrumento e seus anexos.	Contrato nº 40/2024, Pregão Eletrônico nº 015/2024, Processo TJ-CON-2023/00404	Assinatura em 16/07/2024	Brasoftware Informática Ltda., CNPJ 57.142.978/0001-05	Quantidade 10.000	R\$ 19.972.800,00
				Valor Unit. Mensal R\$ 55,48	

* Observação: o valor informado refere-se exclusivamente ao item 5 do Contrato nº 40/2024, correspondente ao SKU AAA-10732, EMS E3, com quantidade de 10.000 licenças, preço unitário de R\$ 55,48 e valor global do item de R\$ 19.972.800,00. Não corresponde ao valor total do contrato, que contempla diversos outros itens e serviços Microsoft.



Órgão 5 - Agência Nacional de Transportes Aquaviários

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAD-33204	PREÇO TOTAL DO CONTRATO (12 meses)
Contratação de subscrição de licenças de uso de softwares Microsoft, pelo período de 12 (doze) meses, para ambiente corporativo e datacenter da Agência Nacional de Transportes Aquaviários, com o respectivo fornecimento de licenças, suporte e benefícios, nas condições estabelecidas no Termo de Referência, anexo do Edital.	Contrato Administrativo nº 07/2024, Processo nº 50300.010387/2023-09	Assinatura em 02/05/2024	Brasoftware Informática Ltda., CNPJ 57.142.978/0001-05	Quantidade 620	R\$ 1.207.586,40
				Valor Unit. Mensal R\$ 162,31	

* Observação: o valor informado refere-se exclusivamente ao item 1 do Contrato nº 07/2024, correspondente ao SKU AAD-33204, M365 E3 UNIFIED SUB PER USER, com quantidade de 620 licenças, preço unitário de R\$ 162,31 e valor global do item de R\$ 1.207.586,40. Não corresponde ao valor total do contrato, que contempla diversos outros itens e serviços Microsoft.

Órgão 6 - Tribunal Regional Federal da 3ª Região

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	AAD-33204	PREÇO TOTAL DO CONTRATO (12 meses)
Contratação de empresa especializada para o fornecimento da renovação de subscrições Microsoft no regime Enterprise Agreement Subscription (EAS), e créditos de serviços por um período de 36 meses, conforme quantidades e especificações constantes do Termo de Referência	CONTRATO Nº 05.022.10.2023	Assinatura em 21/11/2023	PTLS SERVIÇOS DE TECNOLOGIA E ASSESSORIA TÉCNICA LTDA - FILIAL	Quantidade 100	R\$ 2.398.848,00
				Valor Unit. Mensal R\$ 1.999,04	

* Observação: o valor informado refere-se exclusivamente ao item 1.4 do Contrato nº 05.022.10/2023, correspondente ao SKU AAD-33204, M365 E3 UNIFIED SUB PER USER, com quantidade de 100 licenças, preço unitário de R\$ 1.999,04 e valor global do item de R\$ 2.398.848,00. Não corresponde ao valor total do contrato, que contempla diversos outros itens e serviços Microsoft.



Órgão 7 - Secretaria de Estado de Planejamento e Gestão de Minas Gerais - SEPLAG/MG

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO (12 meses)
Contratação de serviços de SERVIÇOS DE SOFTWARES DE LICENÇA MICROSOFT, que serão prestados nas condições estabelecidas no Termo de Referência	Ata de Registro de Preços nº 306/2023-I, Pregão Eletrônico nº 229/2023, Processo SEI nº 1500.01.0138952/2023-05	Assinatura em 08/03/2024	Lanlink Soluções e Comercialização em Informática S/A, CNPJ 19.877.285/0001-71	Quantidade/Horas 600	R\$ 81.804,00
				Valor Unit. R\$ 136,34	



Órgão 8 - Agência Estadual de Tecnologia da Informação de Pernambuco - ATI/PE

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO (12 meses)
Serviços técnicos especializados no desenvolvimento, implementação e sustentação de soluções das plataformas Microsoft	Contrato nº 029/2024, 1º Termo de Apostilamento, adesão à ARP nº 306/2023-I da SEPLAG/MG, Pregão Eletrônico nº 229/2023	Assinatura em 17/12/2024	Lanlink Soluções e Comercialização em Informática S/A, CNPJ 19.877.285/0001-71	Quantidade/Horas 10.000	R\$ 1.363.400,00
				Valor Unit. R\$ 136,34	



Órgão 9 - Tribunal de Contas do Estado do Rio Grande do Sul - TCE/RS

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO (36 meses)
Contratação de serviços técnicos especializados pelo período de 36 (trinta e seis) meses, conforme condições e exigências estabelecidas neste instrumento, no Edital que lhe deu origem, incluindo seus anexos, especialmente o Anexo I – Termo de Referência, bem como na proposta da Contratada.	Contrato nº 50/2025, Pregão Eletrônico nº 08/2025	Assinatura em 03/10/2025	Lanlink Soluções e Comercialização em Informática S/A, CNPJ 19.877.285/0001-71	Quantidade 500 horas/ano	R\$ 315.000,00
				Valor Unit. R\$ 210,00	



Órgão 10 - Tribunal de Contas do Estado do Rio Grande do Norte - TCE/RN

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	FASE / DATA	EMPRESA VENCEDORA	SERVIÇOS TÉCNICOS ESPECIALIZADOS NO DESENVOLVIMENTO, IMPLEMENTAÇÃO E SUSTENTAÇÃO DE SOLUÇÕES DAS PLATAFORMAS MICROSOFT	PREÇO TOTAL DO CONTRATO (12 meses)
Formação de Ata de Registro de Preços para eventual aquisição de licenças Microsoft Office 365 E1, E3, E5 e M365 Copilot pelo período de 36 (trinta e seis) meses, bem como serviços técnicos especializados para migração de e-mails do sistema Zimbra para o Microsoft 365 e treinamento da equipe.	Pregão Eletrônico nº 05/2025	Assinatura em 11/08/2025	TELEFÔNICA BRASIL S.A, CNPJ 02.558.157/0135-74	Quantidade/horas 1.000	R\$ 153.580,00
				Valor Unit. R\$ 153,58	

3.3. Orçamento Estimado

3.3.1. A elaboração do orçamento estimado tomou por base contratações públicas similares celebradas por órgãos da Administração Pública, restritas, para fins de comparabilidade, aos itens de mesmo código de produto (SKU) e, no caso dos serviços, a serviços técnicos de mesma natureza, mensurados por hora. A comparação observou estrita pertinência de objeto, vedado o cotejo entre itens não compatíveis.

3.3.2. Os preços coletados, por se referirem a datas distintas, foram atualizados a valor presente até a data-base adotada nesta análise, conforme a metodologia detalhada no item 8.1.5. A composição das cestas de preços, por item, é a que segue.

Item AAA-10732, Enterprise Mobility + Security E3 (EMS E3), valor por licença ao mês:

Órgão	Instrumento e data	Valor unit. mensal (R\$)	Fator ICTI	Valor presente em 08/09/2025 (R\$)	Situação
SEPLAG/MG (objeto da adesão)	ARP 211/2025 29/08/2025	42,63	-	42,63	Data-base (valor nominal)
Senado Federal	Contrato 12/2025 22/01/2025	48,04	1,020346	49,02	Corrigido
TJBA	Contrato 40/2024 16/07/2024	55,48	1,054521	58,50	Corrigido
MPPA	1º TA à ARP 015/2024 11/09/2025	1.991,79	-	1.991,79	Posterior à data-base (nominal)

Item AAD-33204, Microsoft 365 E3, valor por licença ao mês:

Órgão	Instrumento e data	Valor unit. mensal (R\$)	Fator ICTI	Valor presente em 08/09/2025 (R\$)	Situação
SEPLAG/MG (objeto da adesão)	ARP 211/2025 29/08/2025	176,61	n/a	176,61	Data-base (valor nominal)
ANTAQ	Contrato 07/2024 02/05/2024	162,31	1,069319	173,56	Corrigido
TRF3	Contrato 05.022.10/2023	1.999,04	1,095300	2.189,55	Corrigido

Órgão	Instrumento e data	Valor unit. mensal (R\$)	Fator ICTI	Valor presente em 08/09/2025 (R\$)	Situação
	21/11/2023				

Serviços técnicos especializados em desenvolvimento, implementação e sustentação de soluções, valor por hora técnica:

Órgão	Instrumento e data	Valor unit. hora (R\$)	Fator ICTI	Valor presente em 08/09/2025 (R\$)	Situação
SEPLAG/MG (objeto da adesão)	ARP 211/2025 29/08/2025	140,00	-	140,00	Data-base (valor nominal)
SEPLAG/MG	ARP 306/2023-I 08/03/2024	136,34	1,080247	147,28	Corrigido
ATI/PE	Adesão ARP 306/2023-I 17/12/2024	136,34	1,024957	139,74	Corrigido
TCE/RN	PE 05/2025 11/08/2025	153,58	1,002429	153,95	Corrigido
MPPA	1º TA ARP 015/2024 11/09/2025	141,00	-	141,00	Posterior à data-base (nominal)
TCE/RS	PE 08/2025 03/10/2025	210,00	-	210,00	Posterior à data-base (nominal)

3.4. Da Metodologia de Cálculo para Custo Estimado

- 3.4.1. Os preços das contratações utilizadas como parâmetro foram celebrados em datas diversas. Para assegurar a comparabilidade exigida na formação do preço de referência, os valores dos contratos anteriores foram atualizados a valor presente, da respectiva data de assinatura até a data-base adotada nesta análise.
- 3.4.2. Adotou-se como data-base a data de homologação da Ata de Registro de Preços nº 211/2025 da SEPLAG/MG, em 08/09/2025, uma vez que, até esse marco, o preço registrado não sofreu qualquer reajuste. Por essa razão, o preço da SEPLAG/MG foi considerado em seu valor nominal homologado, sem atualização, servindo de referência fixa do confronto, sendo trazidos a valor presente apenas os preços dos demais órgãos.

- 3.4.3. A pesquisa de preços observou a Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, que disciplina o procedimento de pesquisa de preços para aquisição de bens e contratação de serviços. O art. 5º, inciso I, do referido normativo, ao tratar da composição de custos unitários a partir dos sistemas oficiais de governo, determina seja observado o índice de atualização de preços correspondente, do que se extrai a diretriz de que preços coletados em datas distintas devem ser tornados comparáveis mediante atualização. Com fundamento nessa diretriz, e no art. 6º, §1º, da mesma Instrução Normativa, que admite a adoção de outros critérios ou métodos desde que justificados nos autos, adotou-se a atualização dos preços paradigmas a valor presente, de modo a neutralizar o efeito do tempo e preservar a fidedignidade do referencial de mercado, em harmonia com o art. 23 da Lei nº 14.133/2021
- 3.4.4. Como índice de atualização utilizou-se o Índice de Custos de Tecnologia da Informação (ICTI), por refletir, de forma específica, a evolução dos custos do setor de tecnologia da informação, mostrando-se mais aderente ao objeto desta contratação do que índices gerais de preços. Os índices anuais fechados aplicados foram os seguintes:

Ano	ICTI acumulado	Período de referência
2021	5,74%	Janeiro a dezembro
2022	7,43%	Janeiro a dezembro
2023	1,17%	Janeiro a dezembro
2024	7,26%	Janeiro a dezembro
2025	3,37%	Janeiro a dezembro

- 3.4.5. A atualização foi processada *pro rata*, mês a mês, da data de assinatura de cada contrato até a data-base de 08/09/2025. Cada índice anual fechado foi convertido em taxa mensal equivalente, pela expressão $(1 + i)$ elevado a $(1 \text{ dividido por } 12)$, menos 1, e aplicado proporcionalmente aos dias decorridos em cada competência, de modo que a fração do mês inicial e a do mês final fossem consideradas na exata proporção do período transcorrido. O fator de atualização de cada contrato corresponde ao produto das taxas mensais equivalentes acumuladas no intervalo, indicado na coluna

“Fator ICTI” das tabelas do item 3.3, o que assegura rastreabilidade integral do cálculo.

3.4.6. Os contratos cuja assinatura ou vigência seja posterior à data-base não foram atualizados, por representarem preços supervenientes, e foram considerados em seus valores nominais, com a circunstância expressamente identificada na coluna “Situação”.

3.4.7. Definido o conjunto de preços a valor presente, a referência de mercado de cada item foi obtida segundo o grau de dispersão da amostra, aferido pelo coeficiente de variação (CV), assim entendido o quociente entre o desvio padrão e a média. Para amostras homogêneas, com CV igual ou inferior a 25%, adotou-se a média aritmética. Para amostras com dispersão elevada, com CV superior a 25%, adotou-se a mediana, por ser medida menos sensível a valores extremos e mais representativa do conjunto. Registra-se que as diferenças expressivas observadas entre preços de um mesmo SKU decorrem de variação de mercado, tendo os valores sido verificados em suas fontes oficiais.

3.4.8. O resultado do tratamento estatístico é o que segue:

Item	Média ($\bar{x}$)	Mediana (med)	Desvio padrão (s)	CV (%)	Método recomendado	Valor de referência
AAA-10732 (EMS E3)	R\$ 535,49	R\$ 53,76	R\$ 840,82	157,0%	Mediana	R\$ 53,76
AAD-33204 (M365 E3)	R\$ 846,57	R\$ 176,61	R\$ 949,63	112,2%	Mediana	R\$ 176,61
Serviços técnicos (hora)	R\$ 155,33	R\$ 144,14	R\$ 24,96	16,1%	Média	R\$ 155,33

3.4.9. Os resultados do tratamento estatístico evidenciam que os preços registrados na ARP nº 211/2025 da SEPLAG/MG situam-se, em todos os itens, abaixo do referencial de mercado apurado a valor presente. No item AAA-10732 (EMS E3), **o preço registrado de R\$ 42,63 por licença ao mês representa valor 20,70% inferior à referência de mercado de R\$ 53,76.** No item AAD-33204 (M365 E3), **o preço**

registrado de R\$ 176,61 por licença ao mês corresponde ao mesmo valor de referência de mercado. Nos serviços técnicos especializados, **o preço registrado de R\$ 140,00 por hora situa-se 9,87% abaixo da referência de R\$ 155,33.**

- 3.4.10. A vantajosidade econômica subsiste mesmo após a atualização dos preços paradigmas a valor presente pela aplicação do ICTI, o que afasta a hipótese de que a posição favorável da Ata decorreria da simples defasagem temporal dos contratos comparados. Ao contrário, ainda que neutralizado o efeito do tempo, os preços da SEPLAG/MG permanecem inferiores aos praticados em contratações públicas similares de mesmo objeto.
- 3.4.11. Diante desse cenário, conclui-se que a adesão à ARP nº 211/2025 da SEPLAG/MG é vantajosa para a Administração, por assegurar a contratação dos itens pretendidos a preços comprovadamente inferiores aos de mercado, com a consequente economia de recursos públicos.

3.5. Capacidade e alternativas do mercado de TIC

- 3.5.1. A escolha da solução considera o ambiente tecnológico já implantado no Tribunal, majoritariamente padronizado no ecossistema de produtividade e estações de trabalho em uso, de modo que a plataforma de identidade e gerenciamento de dispositivos aderente a esse ambiente integra-se de forma nativa, sem a camada adicional de conectores e de manutenção contínua que uma solução de fornecedor independente exigiria. Essa aderência reduz o esforço de transição, a curva de aprendizado da equipe técnica e os riscos operacionais, sem prejuízo da competitividade, uma vez que o fornecimento das licenças e dos serviços é disputado por ampla base de parceiros certificados, conforme demonstram as contratações públicas similares analisadas neste Estudo. A definição da solução não decorre, portanto, de preferência por marca, mas de fatos objetivos do parque tecnológico existente, ficando a demonstração de sua vantajosidade técnica e econômica desenvolvida nos itens próprios deste Estudo.

3.6. Contratações correlatas e/ou interdependentes

3.6.1. Não se aplica.

3.7. Escolha e Justificativa da Solução

3.7.1. Descrição da Solução Escolhida (Solução 3)

Concluída a análise comparativa das alternativas e demonstrada a vantajosidade econômica nos itens anteriores, elege-se a Solução 3, consistente na adoção de plataforma de gestão de identidade e acesso integrada nativamente ao gerenciamento unificado de endpoints, ofertada em nuvem e pertencente ao mesmo ecossistema de produtividade e correio eletrônico já utilizado pelo Tribunal. A escolha recai sobre a alternativa que reúne, em um único serviço e sobre uma única base de identidade, as duas camadas que a necessidade institucional trata como indissociáveis: o controle de acessos e o gerenciamento dos dispositivos a partir dos quais esses acessos são exercidos.

A solução entrega, de forma nativa, diretório de identidades unificado para usuários, grupos, dispositivos, aplicações e identidades de serviço, com autenticação única sobre os protocolos abertos SAML 2.0, OAuth 2.0 e OpenID Connect, autenticação multifator com amplo espectro de métodos, acesso condicional avaliado a partir de usuário, dispositivo, localização e nível de risco, detecção de risco de identidade com análise comportamental, gestão de acesso privilegiado e governança do ciclo de vida das identidades, com provisionamento e desprovisionamento automatizados, revisões periódicas e pacotes de acesso. A camada de gerenciamento de dispositivos administra estações e dispositivos móveis a partir de console único em nuvem, sem servidores locais, aplicando políticas de conformidade, inventário, distribuição de configurações, gerenciamento de criptografia de disco e proteção de dados corporativos. A operação conjunta dessas duas camadas materializa uma arquitetura de confiança zero, na qual nenhum usuário ou dispositivo detém confiança implícita e cada solicitação de acesso é avaliada de forma contínua e adaptativa.

A escolha se sustenta por três razões que se reforçam. Tecnicamente, a solução corresponde com exatidão aos requisitos especificados: entrega identidade e gerenciamento de dispositivos de forma integrada, sobre o parque já padronizado no ecossistema institucional, o que garante federação nativa com as aplicações de produtividade e os endpoints em uso, transição de menor risco e menor esforço de sustentação. Some-se a isso a conformidade integral com os normativos do CNJ, atendida de forma nativa em autenticação multifator, gestão centralizada de identidades, controle de acessos baseado em papéis, provisionamento automatizado e revisão periódica de acessos, justamente as lacunas que condenavam o ambiente legado. E, por fim, o custo: os

preços a que a solução pode ser contratada situam-se abaixo do referencial de mercado apurado a valor presente, em todos os itens, conforme a análise comparativa de custos.

A materialização da solução escolhida dá-se por meio da adesão à Ata de Registro de Preços nº 211/2025 da SEPLAG/MG, cujos itens correspondem, com precisão técnica, ao que este Estudo especificou. O item relativo à licença de identidade, gerenciamento de acesso e gerenciamento unificado de dispositivos atende ao perfil da totalidade dos usuários, ao passo que o item relativo à licença que acrescenta a suíte de produtividade e os recursos de colaboração destina-se ao subconjunto de usuários que demandem, além da camada de identidade e dispositivos, a produtividade integrada. A esses soma-se o item de serviços técnicos especializados em desenvolvimento, implementação e sustentação, que assegura a implantação, a integração ao ambiente existente e a sustentação continuada da solução ao longo da vigência contratual, conferindo a capacidade técnica necessária à plena fruição das licenças. As duas licenças assentam-se sobre a mesma base de identidade e sobre o mesmo serviço de gerenciamento de dispositivos, o que garante a coerência arquitetural da solução, com aplicação uniforme das políticas de autenticação multifator, acesso condicional, auditoria e proteção de dados a todos os perfis, sem fragmentação da identidade. Por reunir adequação técnica, conformidade normativa integral, sustentação especializada e vantajosidade econômica, a Solução 3, materializada pela referida adesão, constitui a alternativa mais vantajosa para a Administração.

3.8. Benefícios Esperados

A contratação unifica o controle de acessos do Tribunal sobre uma base única de identidade, superando a fragmentação atual, em que a gestão centralizada alcança apenas o 2º Grau de Jurisdição, enquanto as Comarcas de 1º Grau operam com autenticação local e desarticulada. Como resultado, magistrados, servidores, colaboradores, estagiários e terceirizados passam a operar sob uma identidade corporativa única, com aplicação uniforme das políticas de autenticação multifator, acesso condicional e auditoria em toda a instituição, incluídas as unidades hoje desprovidas de gestão centralizada de acessos.

A solução eleva a postura de segurança ao substituir o modelo de confiança implícita, próprio do diretório legado, pela avaliação contínua e adaptativa de cada solicitação de acesso, considerados usuário, dispositivo, localização e nível de risco. Considerando que o comprometimento de credenciais figura entre os principais vetores de incidente, a autenticação multifator nativa, o acesso condicional, a detecção de comportamento anômalo

e a gestão de acesso privilegiado atuam diretamente sobre a vulnerabilidade mais relevante do ambiente atual, sem a dependência de integrações entre fornecedores distintos que ampliariam a superfície de falha.

A conformidade com os normativos aplicáveis é atendida de forma nativa pela solução, que entrega autenticação forte, controle de acessos baseado em papéis, provisionamento e desprovisionamento automatizados e revisão periódica de acessos, além de favorecer a observância da Lei Geral de Proteção de Dados, com trilha de auditoria apta a sustentar a demonstração perante os órgãos de controle. Os controles que antes dependiam de procedimentos manuais e compensatórios, sujeitos a falha, passam a ser assegurados pela própria arquitetura da plataforma.

A automação do ciclo de vida das identidades reduz, simultaneamente, risco e custo operacional. A vinculação do provisionamento e da revogação de acessos aos eventos de admissão, movimentação e desligamento elimina a janela de acesso residual indevido e desonera a equipe técnica das tarefas repetitivas, permitindo seu redirecionamento para atividades de governança. A aderência da solução ao parque tecnológico já padronizado reduz o esforço de integração e a curva de aprendizado da equipe e viabiliza transição gradual e de menor risco a partir do ambiente existente.

Por ser ofertada em nuvem, a solução incorpora atualização contínua de funcionalidades e de inteligência de ameaças, sem servidores locais e sem o risco de obsolescência e descontinuidade que caracteriza o ambiente legado, de modo que o Tribunal acompanhe a evolução das técnicas de ataque e dos requisitos normativos sem novos ciclos de aquisição. Por fim, as capacidades de registro, auditoria e revisão conferem à Administração visibilidade rastreável sobre os acessos concedidos, suas condições e seus níveis de privilégio, o que fortalece a governança institucional e subsidia a tomada de decisão em matéria de segurança da informação.

3.9. Resultados Esperados

Tipo	Detalhamento
Ganho de Produtividade	A automação do ciclo de vida das identidades, com provisionamento e desprovisionamento vinculados aos eventos de admissão, movimentação e desligamento, elimina tarefas manuais e repetitivas hoje executadas pela equipe técnica, reduzindo o tempo de atendimento dessas demandas e permitindo que os servidores concentrem sua atuação em atividades de planejamento e governança de identidade e acessos.
Redução de Esforço Operacional	A administração unificada de identidades e dispositivos em console único, sem servidores locais, suprime a necessidade de operar e manter mecanismos de autenticação distintos entre os perfis e as unidades. A aderência ao parque tecnológico existente reduz o esforço de integração e de sustentação e dispensa as camadas de conectores que uma solução de fornecedor independente exigiria.
Melhoria na Segurança e Conformidade	A autenticação multifator nativa, o acesso condicional baseado em contexto e risco, a detecção de comportamento anômalo e a gestão de acesso privilegiado, sob a lógica de confiança zero, reduzem a superfície de ataque e o risco de comprometimento de credenciais. A solução atende de forma nativa aos normativos do CNJ em matéria de gestão de identidade e controle de acessos e favorece a observância da LGPD.
Aumento da Confiabilidade das Informações	O registro e a auditoria de todos os eventos de acesso, de forma rastreável, asseguram a integridade e a fidedignidade das informações sobre quem acessa o quê, em que condições e com qual nível de privilégio, fornecendo insumos consistentes para auditorias internas e externas e para a tomada de decisão.
Continuidade dos Serviços Críticos	A unificação do controle de acessos sobre base única de identidade e a substituição do ambiente legado, exposto a risco de descontinuidade e obsolescência, reduzem a probabilidade de indisponibilidade decorrente de falhas de autenticação, assegurando o acesso contínuo e seguro dos magistrados, servidores e demais usuários aos sistemas institucionais.
Redução de Riscos Reputacionais	O fortalecimento dos controles de identidade e acesso mitiga a ocorrência de incidentes que possam resultar em acesso indevido ou em exposição de dados sensíveis, preservando a credibilidade institucional do TJES perante a sociedade e os órgãos de controle.

Transparência e Governança	As capacidades de auditoria, revisão periódica de acessos e geração de relatórios conferem à Administração visibilidade sobre os acessos concedidos e seus níveis de privilégio, assegurando transparência e fortalecendo os mecanismos de governança digital do Tribunal.
----------------------------	--

3.10. Relação entre a Demanda Prevista e a quantidade de bens e/ou serviços contratados

Lote	Item	Descrição	CATMAS	Unidade	Qtd unitária (mensal) [A]	Qtd unitária (36 meses) [B = A * 36]
1	1	Subscrição de licença EMS E3, SKU AAA-10732, (Enterprise Mobility + Security E3), identidade, controle de acesso e gerenciamento unificado de dispositivos, por usuário	112879	Licença	8.500	306.000
	2	Subscrição de licença M365 E3, SKU AAD-33204, (Microsoft 365 E3), identidade, controle de acesso, gerenciamento de dispositivos e produtividade integrada, por usuário	113603	Licença	500	18.000
	3	Serviços técnicos especializados em desenvolvimento, implementação e sustentação das soluções, por hora técnica	126403	Hora	Sob Demanda	2.000

3.11. Estimativa do Custo Total da Solução Escolhida

Lote	Item	Descrição	Unidade	Qtd unitária (mensal) [A]	Qtd unitária (36 meses) [B = A * 36]	Valor unitário (mensal) [C]	Valor total (mensal) [D = A * C]	Valor total (12 meses) [E = D * 12]	Valor total (36 meses) [F = B * C]
1	1	Subscrição de licença EMS E3, SKU AAA-10732, identidade, controle de acesso e gerenciamento unificado de dispositivos, por usuário (valor mensal por licença)	Licença	8.500	306.000	R\$ 42,63	362.355,00	4.348.260,00	13.044.780,00
	2	Subscrição de licença M365 E3, SKU AAD-33204, identidade, controle de acesso, gerenciamento de dispositivos e produtividade integrada, por usuário (valor mensal por licença)	Licença	500	18.000	R\$ 176,61	88.305,00	1.059.660	3.178.980,00



	3	Serviços técnicos especializados em desenvolvimento, implementação e sustentação das soluções (valor por hora técnica)	Hora	Sob Demanda	2.000	R\$ 140,00	Sob Demanda	Sob Demanda	280.000,00
TOTAL GLOBAL									16.503.760,00

3.12. Do pagamento Anual

- 3.12.1. O pagamento das licenças por subscrição ocorrerá de forma anual, em 01 (uma) parcela correspondente a cada período de 12 (doze) meses, considerando o quantitativo de licenças efetivamente contratado e disponibilizado pela CONTRATADA.
- 3.12.2. A primeira parcela será devida após o recebimento e a ativação das licenças no ambiente institucional do CONTRATANTE, mediante aceite da unidade competente, e as demais parcelas serão pagas a cada 12 (doze) meses, durante a vigência contratual, observadas as condições fiscais, orçamentárias e contratuais aplicáveis.

4. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação, após a conclusão dos estudos técnicos preliminares, declara ser viável e adequada a contratação pretendida.

Os estudos demonstraram que a solução escolhida atende integralmente aos requisitos técnicos especificados, mostra-se aderente ao parque tecnológico existente e assegura a conformidade com os normativos do CNJ aplicáveis à gestão de identidade e ao controle de acessos, suprimindo as lacunas que inviabilizavam a manutenção do ambiente atual. Restou igualmente demonstrada a vantajosidade econômica, na medida em que os preços a que a solução pode ser contratada situam-se, em todos os itens, abaixo do referencial de mercado apurado a valor presente.

Diante desses fundamentos, **a contratação é considerada viável e a equipe de planejamento manifesta-se pela sua materialização mediante adesão à Ata de Registro de Preços nº 211/2025 da SEPLAG/MG.**

SUSTENTAÇÃO E ESTRATÉGIA DA CONTRATAÇÃO

5. SUSTENTAÇÃO DO CONTRATO

5.1. Adequação do Ambiente

Não é Aplicável

5.2. Recursos Materiais e Humanos

Não é Aplicável

5.3. Continuidade do Fornecimento

Situação	Ação Preventiva / Contingência	Responsável
Encerramento abrupto do contrato decorrente da adesão	Ação de Contingência: por se tratar de evento imprevisto, providenciar nova autorização de fornecimento junto ao órgão gerenciador, dentro do quantitativo e do prazo de validade da ata de registro de preços, ou, na sua impossibilidade, promover contratação emergencial enquanto se viabiliza solução definitiva, de modo a preservar a continuidade das licenças e do controle de acessos.	Seção de Contratação / STI
Expiração da validade da ata de registro de preços da SEPLAG/MG antes da formalização ou da renovação da adesão	Ação Preventiva: monitorar a vigência da ata, que se encerra em 08/09/2026, e formalizar a adesão e as autorizações de fornecimento dentro do seu prazo de validade, acompanhando eventual prorrogação da ata pelo órgão gerenciador.	Equipe de Planejamento da Contratação / Gestor do Contrato
Indeferimento da adesão pelo órgão gerenciador ou recusa do fornecedor beneficiário	Ação de Contingência: diante da negativa do gerenciador ou da ausência de anuência do fornecedor, buscar adesão a outra ata de registro de preços vigente com objeto compatível ou instaurar processo licitatório próprio, observada a tempestividade necessária à continuidade do serviço.	Equipe de Planejamento da Contratação
Esgotamento do quantitativo disponível para adesão na ata	Ação Preventiva: dimensionar adequadamente a demanda no momento da adesão e acompanhar o saldo disponível, observados os limites de adesão por órgão não participante e o limite global da ata, de modo a evitar a indisponibilidade de quantitativo para novas autorizações de fornecimento.	Gestor do Contrato

Esgotamento do contrato pelo término da vigência	Ação Preventiva: iniciar o planejamento da nova contratação com antecedência mínima de 12 (doze) meses do término do contrato, avaliando tempestivamente a adesão a nova ata de registro de preços ou a realização de licitação própria, com tempo hábil para a tramitação processual, a análise técnica e a homologação.	Equipe de Planejamento da Contratação
Esgotamento do contrato pelo término da vigência	Ação de Contingência: caso a nova contratação não seja concluída em tempo hábil, adotar as providências para a prorrogação do contrato vigente, em caráter excepcional e dentro dos limites legais, mediante justificativa técnica e aprovação da autoridade competente, evitada a interrupção do serviço de identidade e controle de acessos.	Gestor do Contrato
Indisponibilidade ou interrupção do serviço em nuvem pelo fornecedor durante a vigência	Ação Preventiva: exigir contratualmente níveis mínimos de serviço e disponibilidade, acompanhar o seu cumprimento pela fiscalização e acionar o suporte e os mecanismos de escalonamento previstos no instrumento contratual.	Gestor e Fiscal do Contrato
Suspensão das subscrições por falta de renovação tempestiva do pagamento anual	Ação Preventiva: controlar o calendário dos pagamentos anuais das subscrições e providenciar, com antecedência, o empenho e o pagamento das parcelas, de modo a evitar a suspensão das licenças por inadimplência.	Gestor do Contrato

5.4. Transição Contratual e Encerramento do Contrato

- 5.4.1. Por se tratar de fornecimento de licenças de subscrição, mediante adesão a Ata de Registro de Preços, não há transição de equipe, de infraestrutura ou de serviços continuados a ser realizada ao término do contrato.
- 5.4.2. No encerramento, por término da vigência ou por rescisão, a CONTRATADA deverá desvincular eventuais acessos administrativos de que disponha e abster-se de reter dados, registros ou credenciais. Para assegurar a continuidade do licenciamento, a nova contratação deverá ser planejada com a antecedência necessária à sua formalização antes do término do contrato vigente.

5.5. Ações para o Encerramento Contratual

Ação	Responsável	Prazo
Planejamento da nova contratação destinada à continuidade do licenciamento	Equipe de Planejamento da Contratação	Com antecedência mínima necessária à formalização antes do término do contrato vigente
Desvinculação de eventuais acessos administrativos detidos pela CONTRATADA	Contratada	Ao final do contrato
Devolução de credenciais e informações necessárias à administração do ambiente pelo CONTRATANTE, vedada a retenção de dados ou registros	Contratada	Ao final do contrato
Verificação do encerramento das subscrições e da regularidade dos pagamentos das parcelas devidas até o término da vigência	Gestor do Contrato	Ao final do contrato
Emissão do termo de encerramento do contrato	Gestor do Contrato	Após a conclusão das ações anteriores

5.6. Estratégia de Independência Tecnológica

- 5.6.1. Por se tratar de fornecimento de licenças de subscrição mediante adesão à ARP, a independência tecnológica em relação à empresa fornecedora é assegurada pela própria natureza da contratação. O direito de uso das licenças e a operação do ambiente não dependem da fornecedora para subsistir, de modo que a sua substituição, ao término do contrato ou em nova contratação, não acarreta descontinuidade da solução, podendo o licenciamento ser provido por qualquer empresa apta a comercializá-lo.
- 5.6.2. A fim de preservar essa independência, não serão estabelecidos vínculos operacionais que tornem o Tribunal dependente da fornecedora para a administração cotidiana do ambiente, cabendo à equipe técnica do CONTRATANTE manter o controle das configurações e da gestão das identidades e dos acessos.

- 5.6.3. Os serviços técnicos especializados eventualmente acionados deverão ser acompanhados de documentação e repasse de informações à equipe do CONTRATANTE, de modo que as configurações, integrações e customizações implementadas fiquem documentadas e possam ser mantidas e evoluídas independentemente da fornecedora.
- 5.6.4. Ao término do contrato, a CONTRATADA deverá repassar ao CONTRATANTE as informações necessárias à continuidade da administração do ambiente, incluindo, no mínimo, a relação de contas, perfis de acesso e permissões administrativas vinculadas ao fornecimento, bem como a documentação das configurações e integrações realizadas no âmbito dos serviços técnicos prestados.

5.7. Encerramento Abrupto do Contrato

- 5.7.1. Em caso de encerramento abrupto do contrato, por rescisão e independentemente de sua motivação, a CONTRATADA deverá assegurar a manutenção das licenças já contratadas e ativas até o término dos respectivos períodos de subscrição, bem como desvincular eventuais acessos administrativos de que disponha e abster-se de reter dados, credenciais ou registros, de modo a preservar a continuidade da operação do ambiente pelo CONTRATANTE.
- 5.7.2. Verificada a hipótese, o CONTRATANTE adotará as providências de contingência cabíveis para a continuidade do licenciamento, mediante nova autorização de fornecimento no âmbito da ata de registro de preços, enquanto vigente, ou por meio de nova contratação.

6. ESTRATÉGIA PARA A CONTRATAÇÃO

6.1. Natureza do Objeto

O objeto consiste no fornecimento de licenças de subscrição Microsoft, especificamente Enterprise Mobility + Security E3 (EMS E3, SKU AAA-10732) e Microsoft 365 E3 (SKU AAD-33204), destinadas à gestão de identidade, ao controle de acessos e ao gerenciamento unificado de dispositivos, acompanhado de serviços técnicos especializados em desenvolvimento, implementação e sustentação das soluções das plataformas

Microsoft, a ser provido mediante adesão à Ata de Registro de Preços nº 211/2025 da SEPLAG/MG, na condição de órgão não participante.

As licenças de subscrição, em razão de sua validade continuada ao longo da vigência contratual, classificam-se como fornecimento de natureza continuada, necessário à manutenção ininterrupta do controle de acessos do Tribunal. Os serviços técnicos especializados, mensurados por hora técnica e prestados sob demanda específica e eventual, não possuem natureza continuada, esgotando-se na execução de cada atividade requisitada.

Por se caracterizar como bem e serviço comum, com padrões de desempenho e qualidade objetivamente definidos por especificações usuais de mercado, o objeto comporta a contratação por adesão à referida ata de registro de preços, decorrente de pregão eletrônico, dispensada a realização de novo certame, observados os requisitos e os limites da legislação de regência.

6.2. Parcelamento do Objeto e Adjudicação

Por se tratar de adesão à Ata de Registro de Preços nº 211/2025 da SEPLAG/MG, não há que se falar em parcelamento ou em adjudicação, matérias afetas ao certame já realizado pelo órgão gerenciador. A adesão observará a estrutura de itens e a forma de adjudicação definidas na ata, limitando-se o Tribunal a aderir aos itens correspondentes à sua necessidade.

6.3. Subcontratação

Não haverá subcontratação.

6.4. Do Consórcio

Não se aplica.

6.5. Modalidade e Tipo da Licitação

Não haverá realização de licitação por parte do Tribunal, uma vez que a contratação se dará por adesão à Ata de Registro de Preços nº 211/2025 da SEPLAG/MG.

6.6. Vigência do Contrato

- 6.6.1. O contrato terá vigência de 36 (trinta e seis) meses, contados de sua assinatura.
- 6.6.2. A definição do prazo de 36 (trinta e seis) meses guarda coerência com o modelo de licenciamento por subscrição, cujo pagamento é

realizado anualmente, e com a estimativa de custo e os quantitativos definidos neste Estudo. Eventual prorrogação observará a natureza continuada do fornecimento das licenças e os limites e requisitos da legislação de regência, condicionada à verificação da vantajosidade para a Administração e à vigência da ata de registro de preços ou de instrumento que a suceda.

6.7. Equipe de Apoio à Contratação

Integrante Demandante: Teófilo Teixeira Dias

Email: ttdias@tjes.jus.br

Integrante Técnico: Jeferson Kretli Mendes

Email: jkmendes@tjes.jus.br

Integrante Administrativo: David Sudre de Andrade

Email: dasandrade@tjes.jus.br

Integrante Administrativo: Márcio Flávio Barbosa de Souza

Email: mafsouza@tjes.jus.br

7. Equipe de Gestão do Contrato

Gestor Titular: Robson Limaverde Valenca da Silva

Email: rlsilva@tjes.jus.br

Gestor Substituto: Karina Marques Pereira

Email: [kmpereira@tjes.jus.br](mailto:kmperreira@tjes.jus.br)

Fiscal: Klaus Kly Cozzuolo Wolff Mischiatti

Email: kkmischiatti@tjes.jus.br

8. ANÁLISE DE RISCOS

8.1. Riscos Mapeados

Risco 01	Risco:		Demora no trâmite do processo de adesão, na forma da norma correlata
	Probabilidade:		Alta
	Impacto:		Médio
	Dano 1:		Atraso na contratação do objeto e na disponibilização das licenças
	Tratamento:		Acompanhar
	Id	Ação Preventiva	Responsável
	01	Acompanhar a tramitação processual e cumprir tempestivamente os prazos das etapas de instrução da adesão	Setores envolvidos na contratação
	Id	Ação de Contingência	Responsável
	01	Diligenciar junto aos setores competentes o cumprimento dos prazos e priorizar a instrução do processo	Setores envolvidos na contratação

Risco 02	Risco:		Expiração da validade da ata de registro de preços antes da formalização da adesão
	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Impossibilidade de adesão e necessidade de nova solução de contratação
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Monitorar a vigência da Ata de Registro	Equipe de Planejamento da

		de Preços nº 211/2025 da SEPLAG/MG e formalizar a adesão dentro do seu prazo de validade	Contratação
	Id	Ação de Contingência	Responsável
	01	Buscar adesão a outra ata vigente com objeto compatível ou instaurar contratação própria	Equipe de Planejamento da Contratação

Risco 03	Risco:		Indeferimento da adesão pelo órgão gerenciador ou recusa do fornecedor beneficiário
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Inviabilização da contratação pretendida pela via da adesão
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Consultar previamente o órgão gerenciador e o fornecedor quanto ao interesse e à disponibilidade de quantitativo antes de instruir a adesão	Equipe de Planejamento da Contratação
	Id	Ação de Contingência	Responsável
	01	Buscar adesão a outra ata vigente com objeto compatível ou instaurar contratação própria	Equipe de Planejamento da Contratação

Risco	Risco:	Esgotamento do quantitativo disponível para
--------------	---------------	---

04			adesão na ata
	Probabilidade:		Baixa
	Impacto:		Médio
	Dano 1:		Indisponibilidade de quantitativo para atender integralmente à demanda
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Dimensionar a demanda e confirmar o saldo disponível na ata antes da adesão, observados os limites de adesão por órgão não participante	Gestor do Contrato
	Id	Ação de Contingência	Responsável
	01	Complementar a demanda por adesão a outra ata ou por contratação própria	Equipe de Planejamento da Contratação

Risco 05	Risco:		Atraso na disponibilização das licenças pelo fornecedor
	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Atraso no início da operação e na implantação do controle de acessos
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Estabelecer prazos de entrega no contrato e acompanhar o seu cumprimento desde a assinatura	Gestor e Fiscal do Contrato

	Id	Ação de Contingência	Responsável
	01	Notificar o fornecedor para regularização e aplicar as sanções contratuais cabíveis	Gestor do Contrato

Risco 06	Risco:		Indisponibilidade ou interrupção do serviço em nuvem pelo fornecedor da plataforma
	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Interrupção do controle de acessos e do acesso dos usuários aos sistemas
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Exigir contratualmente níveis mínimos de serviço e disponibilidade e acompanhar o seu cumprimento	Gestor e Fiscal do Contrato
	Id	Ação de Contingência	Responsável
	01	Acionar o suporte e os mecanismos de escalonamento previstos no contrato e registrar a ocorrência para fins de penalização	Gestor do Contrato

Risco 07	Risco:	Suspensão das subscrições por falta de renovação tempestiva do pagamento anual
-----------------	---------------	--

	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Suspensão das licenças e interrupção do controle de acessos
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Controlar o calendário dos pagamentos anuais e providenciar empenho e pagamento com antecedência	Gestor do Contrato
	Id	Ação de Contingência	Responsável
	01	Regularizar o pagamento com urgência e adotar as medidas de reativação junto ao fornecedor	Gestor do Contrato

Risco 08	Risco:		Dimensionamento inadequado do quantitativo de licenças
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Aquisição de licenças em excesso ou em número insuficiente para a demanda
	Tratamento:		Mitigar
	Id	Ação Preventiva	Responsável
	01	Levantar a demanda com base no quadro funcional e nos perfis de acesso, prevendo flexibilidade de ajuste das quantidades	Equipe de Planejamento da Contratação



Poder Judiciário

Tribunal de Justiça do Estado do Espírito Santo

Secretaria de Tecnologia da Informação e Comunicação

	Id	Ação de Contingência	Responsável
	01	Ajustar o quantitativo de licenças nos marcos contratuais previstos, conforme a movimentação do quadro funcional	Gestor do Contrato

APROVAÇÃO E ASSINATURA

Equipe de Planejamento da Contratação, instituída pelo Ato nº 166/2026, de 29 de junho de 2026, bem como pela autoridade competente da área de TIC, aprovam o Estudo Técnico Preliminar (ETP) e atestam sua conformidade às disposições da Resolução CNJ nº 468/2022.

Integrante Demandante: Teófilo Teixeira Dias
Email: ttdias@tjes.jus.br

Integrante Técnico: Jeferson Kretli Mendes
Email: jkmendes@tjes.jus.br

Integrante Administrativo: David Sudré de Andrade
Email: dasandrade@tjes.jus.br

Integrante Administrativo: Márcio Flávio Barbosa de Souza
Email: mafsouza@tjes.jus.br

CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

Confirmo o recebimento do presente estudo, no qual tomo ciência de forma integral de seu conteúdo.

Para prosseguimento, encaminho à Secretaria Geral para as providências cabíveis.

Secretária (o) de Tecnologia da Informação:

<Assinam este documento o Integrante Demandante, o Integrante Técnico, o Integrante Administrativo, responsáveis pela elaboração do documento (Equipe de Planejamento da Contratação); e o (a) Secretário (a) da área demandante>