



TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 5/2023 - TRE-ES/PRE/DG/STI/CSGIT/SAGGI

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO.

- 1. Caracterização da Demanda.**
- 2. Especificação dos Requisitos Funcionais.**
- 3. Especificação dos Requisitos Tecnológicos.**
- 4. Identificação e Comparação das Soluções Aderentes aos Requisitos.**
- 5. Indicação da STIC Escolhida.**
- 6. Indicação da Necessidade de Adequação Ambiental**

ANÁLISE DE RISCOS.

- 7. Identificação dos Riscos.**
- 8. Relação dos Riscos e Ações de Mitigação.**

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO.

- 9. Recursos Materiais e Humanos.**
- 10. Descontinuidade do Fornecimento.**

Anexo A.

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

[Obrigatório mesmo para prorrogações, art. 19, § único, resolução TRE-ES nº 261/2018]

1. CARACTERIZAÇÃO DA DEMANDA

1.1. DESCRIÇÃO SUCINTA

- Contratação da solução integrada de e-mail, ferramentas de escritório e planejamento de tarefas, compartilhamento e armazenamento de arquivos em nuvem, ferramenta de comunicação em vídeo e gerência e administração da solução já utilizado pela instituição e fornecido pela empresa Microsoft (Office 365);
- Ampliação do escopo de licenças para incluir a possibilidade de instalação de aplicações desktop;
- Contratação de soluções com recursos para proteção de contas e dados associados à estas contas homologados pela fabricante da solução.

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

- A evolução tecnológica que vem sendo aplicada ao TRE/ES e as novas necessidades emergentes no que tange a adequação às normas regulamentares impactam diretamente a natureza das tecnologias utilizadas para suportar as funções negociais da instituição. A crescente demanda por entrega eficiente dos serviços necessários ao cumprimento da missão institucional obriga que as atividades que subsidiam o processo negocial sejam cada vez mais eficazes e produzam a resposta desejada.
- Diversos investimentos têm sido realizados no parque computacional, para suportar atividades como Mensageria Eletrônica, hospedagem de sítio interno e externo do Tribunal, aplicações de segurança, aplicações de suporte ao processo eletrônico, bem como a hospedagem das aplicações utilizadas pelas unidades do TRE/ES. O investimento no licenciamento da plataforma Office 365 E1 tem trazido aos usuários do Tribunal a possibilidade de utilização de soluções de tecnologia ágeis e funcionais. Atualmente, estão licenciados 532 usuários na plataforma Office 365 E1, utilizando o pacote Office On-line, Teams, Sharepoint, armazenamento OneDrive, Power Apps e Power Automate.
- A solução visa manter a comunicação entre os servidores, possibilitando localizar o servidor durante o horário de trabalho, além de prover armazenamento em nuvem e várias outras funcionalidades utilizadas. A continuidade da solução deverá manter o ambiente online para os servidores, equivalente à sua estação de trabalho, com e-mail, armazenamento de arquivos e trabalho colaborativo com outros servidores, além de permitir a realização de comunicação em vídeo com qualquer pessoa, a qualquer tempo, possibilitando a troca de informações, compartilhamento de arquivos, reuniões por videoconferência e a elaboração de

planejamento das atividades, previsto na Resolução TRE/ES n. 266/2020, que regulamenta a nova forma de gestão do trabalho presencial e remoto do Tribunal.

4. Considerando que o Office 365 é hoje a base da solução de produtividade organizacional e trabalho colaborativo do Tribunal, onde trafega-se a armazena-se a grande maioria das informações corporativas, incluindo dados pessoais e dados sensíveis é de suma importância que a equipe de segurança conte com os recursos de proteção avançada oferecidos pela fabricante para garantir a integridade, privacidade e disponibilidade destas informações. A equipe de segurança considera que os recursos básicos presentes no EOP (Exchange Online Protection) fornecem um grau razoável de segurança, mas enxerga que alguns recursos presentes no Plano 1 do Defender for Office 365 são essenciais para o grau de proteção avançado desejado pelo Tribunal.

5. O Azure AD é o serviço de gerenciamento de identidade e acesso baseado em nuvem que sustenta a utilização do M365. A licença do Azure AD Premium (P1 e P2) permite habilitar recursos avançados de gerenciamento e segurança adicionais que não estão presentes na licença básica do Azure AD. O Azure AD gratuito fornece gerenciamento de usuários e de grupos, sincronização de diretório local, relatórios básicos, autoatendimento para alteração de senha e login único no Azure, no Office 365 e em muitos aplicativos SaaS populares.

6. O Azure AD Premium P1, além dos recursos gratuitos, também permite que seus usuários híbridos acessem recursos locais e de nuvem. Ele também dá suporte à administração avançada, como grupos dinâmicos, gerenciamento de grupos de autoatendimento, Microsoft Identity Manager e recursos de write-back de nuvem, que permitem a redefinição de senha por autoatendimento para os usuários locais.

7. O Azure AD Premium P2, além dos recursos nos planos Gratuito e P1, também oferece o Azure Active Directory Identity Protection, a fim de fornecer Acesso Condicional baseado em risco para seus aplicativos e dados críticos da empresa, e o Privileged Identity Management, para ajudar a descobrir, restringir e monitorar os administradores e o acesso deles a recursos e fornecer acesso Just-In-Time quando for necessário.

8. A equipe de segurança entende que alguns recursos fornecidos pelos planos P1 e P2 são fundamentais para atingir o nível de segurança desejado pelo Tribunal. Adicionalmente, recursos como o write-back de nuvem e grupos dinâmicos serão vantajosos para a equipe em termos de gerenciamento.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1. REQUISITOS RELACIONADOS AO NEGÓCIO

1. Continuidade da comunicação entre os servidores por meio de voz, áudio e texto;
2. Continuidade do compartilhamento de arquivos entre os servidores;
3. Continuidade da realização de reuniões online em áudio e vídeo com gravação;
4. Continuidade da realização de tarefas remotas bastando a identificação do usuário e a obtenção de acesso aos recursos em nuvem;
5. Continuidade da realização de tarefas com ferramenta de escritório online;
6. Continuidade do armazenamento de arquivos pessoais em nuvem com acesso compartilhado;
7. Continuidade do controle de acesso aos documentos compartilhados;
8. Continuidade da administração da solução, grupos de trabalho e caixas de correio eletrônico;
9. Continuidade do uso do domínio do Contratante (tre-es.jus.br);
10. Disponibilização para pelo menos 640 usuários;
11. Compatibilidade com as ferramentas já utilizadas pelo Contratante visando a redução do impacto em capacitações e treinamentos;
12. Garantir a segurança de acesso às contas de usuários, aos anexos e aos documentos;
13. Garantir o monitoramento preventivo de ameaças e a detecção de vulnerabilidades.

2.2. REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

1. A ferramenta já se encontra implantada e em operação no TRE/ES, não havendo requisitos de capacitação relacionados;
2. A necessidade de capacitações ou ajustes ambientais relacionados a elementos específicos da solução, deverá ser considerada caso a caso.

2.3. REQUISITOS DE MANUTENÇÃO E GARANTIA

1. Deverá ser fornecido suporte online e por telefone pelo menos nas horas úteis;
2. O serviço deverá possuir disponibilidade de pelo menos 99,9%.

2.4. REQUISITOS TEMPORAIS

1. Devem ser permitidas prorrogações de forma a minimizar o impacto de mudanças na instituição, sempre na forma da lei.

2.5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1. O Tribunal compartilhará com a contratada dados pessoais controlados, incluindo, mas não se limitando a: Título Eleitoral, Documento Oficial de Identificação, CPF, E-mail, Endereço, Telefone, Estado Civil, Ocupação (Profissão), entre outros.
2. A contratada terá acesso a informações sensíveis do Tribunal, incluindo, mas não se limitando a: Origem racial ou étnica, filiação a organização sindical, religiosa, filosófica ou política, dados referentes à saúde ou vida sexual, dados genéticos ou biométricos, vídeos e fotografias, entre outros.
3. Assim, é necessário incluir no Termo de Referência o seguinte: a) O MODELO do Termo de Compromisso de Manutenção de Sigilo, a ser assinado pela empresa; b) O MODELO do Termo de Ciência e Aceite do Termo de Compromisso de Manutenção de

Sigilo e do Código de Ética do TRE/ES, a ser assinado por todos os profissionais da contratada que estejam envolvidos no contrato.

4. Os recursos de segurança oferecidos pelo Defender for Office 365 Plan 1 vistos como essenciais pela equipe de segurança são:

- a) **Anexos Seguros para Outlook e Teams** - Fornece proteção avançada contra vírus e malwares “zero day” para todo o sistema de mensagens através de verificação de assinaturas conhecidas e técnicas de *machine learning*.
- b) **Links Seguros para Outlook e Teams** - Fornece proteção proativa contra URLs mal-intencionadas em mensagens de e-mail, documentos do Office ou mensagens do Teams em chats ou canais através do bloqueio dinâmico dos links mal-intencionados.
- c) **Proteção para SharePoint, OneDrive e Microsoft Teams** - Extensão da proteção de Anexos Seguros para todos os arquivos em sites de equipe e bibliotecas de documentos bloqueando o acesso a arquivos mal-intencionados identificados.
- d) **Políticas anti-phishing** - Permite a criação de políticas avançadas de anti-phishing explorando os recursos de proteção fornecidos pelos Anexos Seguros, Links Seguros e modelos de machine learning que analisam as mensagens de entrada em busca de indicadores de tentativa de phishing.
- e) **Deteção em tempo real** - Fornece relatórios detalhados para a equipe de segurança investigar e responder a ameaças com eficiência. Os relatórios permitem analisar malware detectado, examinar URLs apontadas como phishing, verificar e-mails classificados como mal-intencionados.

5. Os recursos adicionais fornecidos pelos planos P1 e P2 vistos como essenciais pela equipe de segurança são:

- a) **Write-back de senha (P1)** - Permite que as alterações de senha realizadas pelos usuários finais na plataforma de nuvem sejam replicadas para o ambiente on-premise.
- b) **Grupos Dinâmicos (P1)** - Permite a atualização automática de grupos com base em regras predefinidas. Essas regras são criadas com base em atributos dos usuários e dispositivos, como departamento, cargo ou localização. Dessa forma, os Grupos Dinâmicos garantem que os usuários recebam automaticamente os acessos e permissões corretos com base nas regras definidas, sem a necessidade de gerenciamento manual.
- c) **Identity Protection (P2)** - Utiliza análise de risco em tempo real para detectar e mitigar riscos de segurança em contas de usuário, como senhas fracas, tentativas de login suspeitas ou atividades incomuns. O Identity Protection também pode ser usado para criar políticas de segurança personalizadas com base em padrões de atividade de usuário, tais como bloquear o acesso de usuários a determinados recursos ou exigir autenticação multifator. Além disso, ele fornece relatórios detalhados sobre atividades de usuários para ajudar a equipe de segurança a identificar e solucionar rapidamente potenciais ameaças.
- d) **Acesso condicional baseado em risco (P2)** - Enquanto as políticas de Acesso Condicional do P1 se concentram principalmente em decidir se um usuário deve ou não ter acesso a um recurso com base em informações estáticas, como localização e hora do dia, o Identity Protection leva em consideração fatores de risco dinâmicos, como tentativas de login suspeitas ou atividades incomuns do usuário. Combinando essas informações com políticas de acesso condicional personalizadas, o Identity Protection pode fornecer um controle de acesso mais granular, garantindo que apenas usuários confiáveis tenham acesso a recursos e dados sensíveis.
- e) **Revisões de acesso (P2)** - Com as revisões de acesso, os administradores podem definir políticas para revisar periodicamente as permissões de acesso e atribuir tarefas de revisão a outros usuários a fim de garantir que os usuários tenham apenas o acesso necessário aos recursos e dados da instituição.
- f) **Privileged Identity Management - PIM (P2)** - Permite gerenciar e controlar o acesso privilegiado a recursos críticos de uma organização, como contas de administrador, chaves de criptografia e outros recursos confidenciais. Com o PIM, pode-se definir funções de administrador, atribuir permissões para essas funções e limitar o tempo de atividade dos usuários nessas funções. Os usuários só têm acesso à função de administrador quando precisam dela e após serem autorizados por um revisor designado. O PIM também permite que as organizações monitorem e auditem as atividades dos usuários com acesso privilegiado.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS MÍNIMOS

3.1. CARACTERÍSTICAS GERAIS

1. Fornecimento de Correio Eletrônico baseado em nuvem;
2. Comunicação via chat e vídeo;
3. Armazenamento de arquivos para trabalho colaborativo em nuvem, movimentação entre equipamentos pessoais e a nuvem;
4. Agenda integrada ao Exchange (correio eletrônico *on premise*);
5. Compartilhamento de arquivos em grupos de trabalho;
6. Sincronização de arquivos em nuvem/computador pessoal/dispositivo móvel;
7. Reuniões e chamadas em grupo com pelo menos 200 pessoas e tempo ilimitado;
8. Gravação de reuniões;
9. Ferramenta de planejamento integrada;
10. Plataforma web para gestão de conteúdo, gestão documental e criação;
11. Elaboração de formulários online;
12. Pacote de ferramentas online de escritório que contemplem:
 1. Edição de documentos em texto com formatações diversas;
 2. Planilhas eletrônicas com limitações de linhas e colunas superiores a 1000 (mil);
 3. Apresentações;
13. Na gestão da solução a ferramenta deve prover:
 1. Administração completa de usuários integrada ao Active Directory (AD da Microsoft);
 2. Administração completa de grupos de trabalho colaborativo;
 3. Administração completa de caixas de correio eletrônico;

4. Possibilidade de manutenção de caixas postais “on premise” no Exchange (ferramenta usada pelo contratante) e caixas postais online integradas;
5. Nome de domínio personalizado para endereços de e-mail;
14. Serviço de compartilhamento de arquivos:
 1. Compartilhamento de arquivos entre os usuários internos;
 2. Criação de ambientes (Intranet) para publicação e compartilhamento em grupos internos;
 3. Compartilhamento para público externo, caso necessário;
15. Requisitos de capacidade deverão ser de no mínimo:
 1. Caixa de correio eletrônico com pelo menos 50GB;
 2. Armazenamento de arquivos com pelo menos 1 TB;
 3. Capacidade de armazenamento de vídeo em, no mínimo, 500GB;
16. Requisitos de Segurança da Informação
 1. Proteção contra vírus e "malwares";
 2. Proteção contra URLs mal-intencionadas em mensagens de e-mail e documentos;
 3. Proteção de Anexos para todos os arquivos em sites de equipe e bibliotecas;
 4. Criação de políticas "anti-phishing";
 5. Detecção em tempo real de ameaças;
 6. Replicação de senhas alteradas no ambiente "on premise";
 7. Atualização dinâmica de grupos;
 8. Análise dinâmica de eventos de acesso;
 9. Controle de acesso baseado em privilégios.

3.2. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

1. A solução adotada trata-se de uma solução baseada em nuvem, mesmo com a dependência tecnológica, usar uma solução em nuvem pode ser vantajosa para a instituição. As soluções em nuvem oferecem várias vantagens, incluindo escalabilidade, acessibilidade, redução de custos, atualizações automáticas, flexibilidade e segurança. Embora exista o risco de dependência tecnológica com soluções em nuvem, o Tribunal pode tomar medidas para mitigar esse risco, como garantir que os dados estejam disponíveis offline, manter backups regulares e implementar planos de continuidade de negócios.
2. Além disso, a dependência tecnológica não é exclusiva das soluções em nuvem. As empresas que utilizam soluções "on premise" também podem enfrentar dependência de tecnologia, como depender de um único fornecedor de hardware ou software. Em última análise, a decisão de usar uma solução em nuvem deve ser baseada nas necessidades específicas do Tribunal e nos riscos e benefícios associados a essa tecnologia.
3. Durante a pandemia da COVID-19, ficou evidente que a solução implementada e as vantagens obtidas superaram os riscos potenciais de dependência tecnológica e interrupções na prestação de serviços jurídicos e eleitorais, pelos quais a instituição é responsável.
4. A instituição do Programa de Gestão de Continuidade de Negócios (PGCN) consta nos itens A054, A055, A056, A057, A058 do Plano de Trabalho de Segurança da Informação e Proteção de Dados, parte do PDTIC 2021-2026. O plano de continuidade é de fundamental importância para o estabelecimento de metas e parâmetros para que a dependência tecnológica seja mitigada.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

4.1. COMPARATIVO ENTRE OPÇÕES

1. Como a solução já se encontra implantada, os impactos de migração para outra solução são inúmeros, pode-se citar:

a) **Diferenças de recursos e funcionalidades:** O Office 365 e a outra solução têm conjuntos de recursos e funcionalidades diferentes. Ao migrar para outra solução, o Tribunal precisará se familiarizar com as ferramentas e recursos específicos oferecidos pela nova plataforma. Isso pode exigir treinamento adicional para os servidores, pois a interface e a forma de trabalhar podem ser diferentes.

b) **Integração e interoperabilidade:** Como o Tribunal já está usando intensivamente recursos do Office 365, como o SharePoint Online, Microsoft Teams ou Power Automate, a migração para outra solução vai exigir uma avaliação cuidadosa da integração com outras ferramentas e sistemas existentes. Seria necessário considerar como essas integrações serão afetadas e se haverá necessidade de adaptações ou substituições de soluções.

c) **Arquivos e dados existentes:** A migração para outra solução exigiria a transferência de arquivos, documentos e outros dados do Office 365 para a nova plataforma. Esse processo pode ser complexo e requerer um planejamento cuidadoso para garantir que todos os dados sejam transferidos corretamente e que não haja perda de informações importantes ou interrupção nas operações.

d) **Interação com outros usuários e instituições:** O Tribunal colabora frequentemente com outras instituições, fornecedores ou eleitores em geral que usam o Office 365, a mudança para outra solução poderia afetar a forma como a colaboração é realizada. Pode ser necessário avaliar a compatibilidade e a capacidade de trabalhar em conjunto usando diferentes plataformas (como por exemplo, o Balcão Virtual, que hoje é totalmente implementado utilizando o Teams).

e) **Custo e investimento:** A migração para outra solução envolve custos, tanto em termos de licenciamento quanto em serviços de migração e treinamento. O Tribunal deve considerar esses custos e avaliar se a mudança resultará em benefícios significativos que justifiquem o investimento.

f) É importante lembrar que cada organização é única, e os impactos específicos de uma migração podem variar dependendo de vários fatores, como o tamanho da instituição, a complexidade dos processos existentes e as necessidades de colaboração e integração com outras empresas. Caso seja necessário uma migração, é recomendado realizar uma avaliação completa dos requisitos, impactos e benefícios antes de tomar a decisão de migrar para outra solução ou qualquer outra plataforma.

g) Considerando os potenciais riscos e implicações mencionados anteriormente, é importante ponderar cuidadosamente sobre os severos impactos na adoção de uma solução diferente do Office 365. São diversos os custos envolvidos em termos de tempo, recursos e treinamento necessários para uma transição suave. Nesse contexto, pode-se concluir que, em praticamente todos os casos, manter a solução atual da Microsoft é uma decisão mais econômica e prática neste momento, especialmente levando em conta a complexidade e os desafios potenciais associados a uma migração completa para outra solução.

4.2. VISÃO GERAL

1. O Office 365 é uma suíte de aplicativos e serviços baseados em nuvem da Microsoft, projetada para aumentar a produtividade e colaboração nas empresas. Ele inclui uma ampla variedade de aplicativos conhecidos, como Word, Excel, PowerPoint e Outlook, que permitem criar, editar e compartilhar documentos, planilhas, apresentações e e-mails. Além disso, oferece recursos avançados, como armazenamento em nuvem com o OneDrive, comunicação e colaboração por meio do Microsoft Teams, gerenciamento de projetos com o SharePoint Online e automação de processos com o Power Automate. Com acesso em qualquer dispositivo e atualizações regulares, o Office 365 proporciona ferramentas poderosas para otimizar fluxos de trabalho, promover a colaboração e facilitar o trabalho em equipe.

2. No quesito “Compatibilidade com as ferramentas já utilizadas pelo Contratante visando a redução do impacto em capacitações e treinamentos” a única solução compatível é a solução fornecida pela Microsoft;

5. INDICAÇÃO DA STIC ESCOLHIDA

5.1. DESCRIÇÃO DA SOLUÇÃO

1. Manutenção da solução Office 365, com a adição de eventuais adendos de segurança e perfis de plano de assinatura.

5.2. JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

1. A solução da Office 365 continua apresentando total compatibilidade com a infraestrutura do Tribunal, integrando ferramentas já adquiridas e utilizadas, como pacote office, servidor de correio Exchange. Em função dessa compatibilidade e de cumprir a função de possibilitar o planejamento de atividades e projetos (item 2.4 da tabela de requisitos), é a única solução que atende integralmente os requisitos funcionais necessários. Importante destacar que a exigência de uma ferramenta de planejamento de atividades e projetos na solução de trabalho colaborativo é essencial para o cumprimento de vários dispositivos da resolução 266/2020, dentre os quais se destacam:

Art. 2º São princípios a serem observados na execução desta Resolução:

II - planejamento;

III - comunicação constante;

Art. 3º Para a implementação do modelo, os gestores deverão:

I - em relação à gestão do trabalho:

a) planejar as atividades da equipe em ciclos sucessivos de duas a quatro semanas, ou de quinze dias a um mês, em sequência ininterrupta;

b) distribuir o trabalho entre os membros da equipe, negociando prazos e qualidade esperados;

c) acompanhar diariamente o trabalho desenvolvido pela equipe com o uso de ferramentas de comunicação online;

II - Em relação à gestão de equipes, estabelecer uma rotina estruturada de trabalho, que inclua:

b) definição de ambiente de comunicação on-line que permita a interação entre os membros da equipe para tratar sobre questões gerais de trabalho, projetos específicos, solução de questões pontuais e para a integração do grupo;

c) definição de ambiente que possibilite aos membros da equipe visualizar o status das atividades previstas, das que estão pendentes, das que estão em execução e das concluídas, e colaborar em sua atualização;

2. As ferramentas Office 365 já são utilizadas há vários anos pelos servidores do TRE/ES, sendo um ativo importante todo esse conhecimento já adquirido pelos usuários e facilitará o aprendizado dos novos recursos online;

3. Principalmente após a adoção do Office 365 E1, a integração das aplicações legadas com os recursos online disponibilizados pela solução aumentou significativamente, o que reforçou ainda mais a recomendação do Office 365.

5.3. ESTIMATIVA DE CUSTO

1. A estimativa anual na solução Office 365 + Azure AD Premium P2 + Defender P1 é de R\$ 660.206,16. Sendo 622 licenças Office 365 E1 e 18 licenças Office 365 E3.

ESTIMATIVA ANUAL				
Nº de licenças:	622	18	0	
Solução	E1	E3	E5	Total
Office 365	R\$ 280.944,96	R\$ 15.843,60	R\$ -	R\$ 296.788,56

Azure AD Premium P2	R\$ 300.426,00	R\$ 8.694,00	R\$ -	R\$ 309.120,00
Defender Plano 1	R\$ 52.770,48	R\$ 1.527,12	R\$ -	R\$ 54.297,60
				R\$ 660.206,16

Fontes: Catálogo de Soluções de TIC com Condições Padronizadas - Microsoft

5.4. ADERÊNCIA AOS REQUISITOS

1. O Office 365 é uma solução abrangente e integrada, que combina várias ferramentas e serviços para aumentar a produtividade e a colaboração no ambiente de trabalho. A solução é baseada na nuvem e inclui uma variedade de aplicativos e recursos projetados para atender inúmeras necessidades. Oferece acesso ao pacote de produtividade do Office, que inclui aplicativos populares como o Word, Excel, PowerPoint, Outlook e outros. Além disso, a solução também inclui recursos de armazenamento e compartilhamento de arquivos online, como o OneDrive, que permite que os usuários acessem seus documentos de qualquer lugar, a qualquer momento. Uma das principais vantagens do Office 365 é a sua capacidade de integração com serviços online e aplicativos de terceiros. Isso significa que os usuários podem aproveitar os recursos de colaboração, como videochamadas, bate-papo, compartilhamento de tela e trabalho simultâneo em documentos, por meio de aplicativos como o Microsoft Teams. Além disso, também oferece recursos avançados de segurança, gerenciamento de dispositivos e conformidade para proteger os dados e manter a conformidade regulatória. A solução é atualizada regularmente com novos recursos e melhorias, garantindo acesso às últimas ferramentas e tecnologias disponíveis.

a) Diferencial entre o plano E1 e o plano E3: O plano E3 possui todos os recursos do plano E1, ou seja, os aplicativos online de produtividade, email, calendário, comunicação e colaboração, armazenamento em nuvem e recursos básicos de conformidade e segurança. Adicionalmente, o plano E3 inclui as versões completas dos aplicativos de área de trabalho do Office, como Word, Excel, PowerPoint e Outlook, permitindo a instalação dos aplicativos localmente e permitindo o trabalho offline.

2. O Microsoft Outlook é um aplicativo de email e gerenciamento de informações pessoais (PIM) da Microsoft, atualmente utilizado pelo Tribunal. Ele oferece recursos avançados para gerenciar emails, calendários e contatos. A integração do Outlook com o Exchange Server, uma solução de email corporativo da Microsoft, permite acesso a contas corporativas, sincronização de dados e colaboração em tempo real, facilitando a comunicação e a produtividade das equipes de trabalho.

3. O Power BI é uma plataforma de análise de dados e business intelligence desenvolvida pela Microsoft. Ele permite que os usuários transformem dados brutos em informações significativas, por meio de recursos avançados de visualização, análise e compartilhamento de dados. Com o Power BI, os usuários podem conectar-se a uma ampla variedade de fontes de dados, incluindo bancos de dados, arquivos locais, serviços em nuvem e até mesmo aplicativos específicos, como o Microsoft Excel. Uma vez conectados, os usuários podem criar painéis interativos, relatórios e gráficos personalizados para visualizar e analisar os dados. Oferece uma ampla gama de recursos de visualização de dados, incluindo gráficos, tabelas dinâmicas, mapas geográficos, medidores, entre outros. Além disso, os usuários podem criar consultas e transformações de dados avançadas por meio do Power Query e modelagem de dados por meio do Power Pivot, permitindo que eles preparem os dados para análise de maneira eficiente. Uma das principais vantagens do Power BI é a sua capacidade de compartilhar insights e colaborar com outras pessoas. Os usuários podem publicar seus relatórios e painéis no serviço do Power BI, permitindo que outras pessoas os acessem e interajam com os dados de forma segura. A ferramenta oferece, ainda, recursos avançados de compartilhamento, como permissões de acesso e atualizações automatizadas de dados, garantindo que os usuários vejam as informações mais recentes. O Office 365, em conjunto com o Power BI, oferece uma solução poderosa para a análise de dados e a tomada de decisões baseada em informações. Ao combinar o poder do Power BI com outros aplicativos e serviços do Office 365, os usuários podem explorar e compartilhar insights de dados de maneira eficiente, impulsionando a produtividade. Atualmente o Tribunal já utiliza a ferramenta.

4. A segurança é uma prioridade fundamental! A Microsoft disponibiliza a Microsoft Azure, uma plataforma de computação em nuvem. O Azure oferece uma variedade de recursos e medidas de segurança para proteger os dados, aplicativos e infraestrutura dos clientes. Possui uma estrutura de segurança robusta, que abrange todos os aspectos da plataforma. Isso inclui a proteção física dos data centers, que são altamente seguros e seguem rígidos protocolos de segurança. Além disso, implementa controles de acesso físico restrito, monitoramento 24/7 e medidas de prevenção e mitigação de riscos. Em termos de segurança de dados, o Azure oferece recursos avançados para proteger as informações. Os dados podem ser criptografados e a plataforma também oferece opções de gerenciamento de chaves e certificados, permitindo aos clientes um controle total sobre seus próprios dados. Fornece recursos de segurança para proteção de identidade e acesso, autenticação multifator e integração com serviços de gerenciamento de identidade, como o Azure Active Directory, permitindo a implementação de autenticação e controle de acesso granular para usuários e recursos. A solução tem foco na detecção de ameaças e a plataforma conta com ferramentas e serviços de segurança avançados, como o Azure Security Center, que analisa e monitora continuamente a infraestrutura em busca de possíveis ameaças. O Azure também oferece recursos de análise de segurança, detecção de anomalias e respostas automatizadas a incidentes de segurança.

5. O Microsoft Teams é uma plataforma de comunicação e colaboração desenvolvida pela Microsoft. Ele permite que indivíduos e equipes se conectem, compartilhem informações, colaborem em projetos e realizem reuniões online, independentemente de sua localização geográfica. O Teams oferece uma variedade de recursos e ferramentas projetados para facilitar a colaboração eficiente. Os usuários podem criar equipes e canais dedicados a projetos específicos, nos quais podem compartilhar mensagens, arquivos e atualizações. Isso ajuda a centralizar as conversas e a manter todos os membros da equipe informados. Além das mensagens instantâneas, o Teams oferece recursos de chamadas de áudio e vídeo, permitindo que os usuários realizem chamadas individuais ou em grupo. As videochamadas podem ser realizadas com áudio e vídeo de alta qualidade, possibilitando reuniões virtuais mais produtivas e interativas. O Teams também permite a colaboração em tempo real em documentos compartilhados. Os usuários podem criar e editar documentos do Microsoft Office, como Word, Excel e PowerPoint, diretamente na plataforma do Teams. Isso possibilita que várias pessoas trabalhem simultaneamente em um documento, facilitando a edição colaborativa e agilizando o processo de criação e revisão de documentos. Uma característica importante do Teams é a integração com outros aplicativos e serviços da Microsoft e de terceiros. Os usuários podem conectar o Teams a aplicativos como o SharePoint, OneDrive, Power BI e muitos outros, permitindo acesso e compartilhamento fácil de dados e informações de diferentes fontes. Além disso, o Teams oferece recursos avançados de organização, como a criação de agendas para reuniões, a atribuição de tarefas e a definição de lembretes. Isso ajuda a gerenciar projetos de forma mais eficiente e manter o controle das atividades e prazos. Em termos de

segurança, o Teams possui recursos robustos para proteger os dados e as comunicações dos usuários. Ele oferece criptografia de ponta a ponta, controle de permissões de acesso, autenticação multifator e conformidade com várias regulamentações de segurança. O TRE/ES implementou o "Balcão Virtual" com absoluto sucesso (<https://www.tre-es.jus.br/servicos-judiciais/balcao-virtual>) e esta solução foi montada utilizando a plataforma Office 365, em particular se utilizando do Microsoft Teams. A ferramenta está sendo utilizada para diversas atividades no Tribunal inclusive para realização de atendimentos à comunidade.

5. O Microsoft OneDrive é um serviço de armazenamento em nuvem fornecido pela Microsoft. Ele permite que os usuários armazenem, sincronizem e compartilhem arquivos e pastas em vários dispositivos, como computadores, tablets e smartphones. O OneDrive oferece aos usuários um espaço de armazenamento online para salvar seus arquivos, que podem incluir documentos, fotos, vídeos e outros tipos de arquivos. Esses arquivos podem ser acessados a partir de qualquer dispositivo com uma conexão à internet, facilitando o acesso e o compartilhamento de informações. Uma das principais vantagens do OneDrive é a integração com outros serviços da Microsoft, como o Windows, o Office 365 e o Outlook.com. Isso permite que os usuários acessem seus arquivos armazenados no OneDrive diretamente de aplicativos como o Word, o Excel e o PowerPoint. Além disso, o OneDrive oferece recursos de colaboração, permitindo que várias pessoas trabalhem simultaneamente em um documento e visualizem as alterações em tempo real. Oferece, ainda, recursos avançados, como a capacidade de restaurar versões anteriores de arquivos, sincronização seletiva (permitindo escolher quais pastas sincronizar em cada dispositivo) e o recurso "Arquivos sob demanda", que permite visualizar e acessar arquivos armazenados no OneDrive sem precisar fazer o download completo deles para o dispositivo local. Os usuários podem acessar o OneDrive por meio de um aplicativo de desktop para Windows e macOS, aplicativos móveis para iOS e Android, bem como pelo navegador da web.

5.5. RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

1. Atualmente, no Tribunal, a distribuição de usuários é mostrado na tabela abaixo.

CATEGORIA	Quantidade
Efetivos	310
Estagiários	28
Juizes Auxiliares	2
Juizes Eleitorais	50
Lotação provisória	2
Membros ativos	12
Removidos para TRE-ES	17
Requisitados	120
Sem vínculo efetivo	8
Terceirizados	39
TOTAL	588
DEMANDA ATUAL DO MS 365	Office 365 E1
Descrição	Quantitativo
Usuários atuais	588
Licenças adicionais para juizes substitutos	10
Licenças adicionais para novos estagiários	32
Licenças adicionais para novos servidores	10
TOTAL	640
LICENÇAS COM INSTALAÇÃO DESKTOP	Office 365 E3
UNIDADE	QUANTIDADE
COF/SECONT	3
COPE/SPSERV	3
COPE/SPAUT	3
COPE/Coordenador	1
CSGIT/SAGGI	3
TÉCNICOS DE SUPORTE	5
TOTAL	18
LICENÇAS MS365 E1	622
LICENÇAS MS365 E3	18

2. Dessa forma, os quantitativos serão distribuídos:

- Office 365 E1, em um total de 622 licenças, **T6A-00024**;
- Office 365 E3, em um total de 18 licenças, **AAA-10906**;
- Microsoft Defender for Office 365 Plan 1, em um total de 640 licenças, **KF5-00002**;
- Microsoft Azure AD Premium P2, em um total de 640 licenças, **6E6-00003**.

5.6 COMPOSIÇÃO DE BENS/SERVIÇOS DA SOLUÇÃO

- Serviço. Software como serviço. Licenças de uso por período determinado, na infraestrutura local ou na nuvem.

2. Software como Serviço (Software as a Service - SaaS) é um modelo de distribuição de software em que um aplicativo é hospedado em servidores de terceiros e disponibilizado aos usuários através da Internet. Em vez de adquirir uma licença de software e instalá-lo localmente, os usuários acessam o software por meio de um navegador da web ou de um cliente dedicado. No modelo SaaS, o fornecedor do software é responsável pela infraestrutura, manutenção, atualizações e segurança do sistema. O pagamento é periódico para utilizar o software. Esse modelo é conhecido por sua abordagem baseada em assinatura.

6. PARCELAMENTO DO OBJETO

1. Não haverá parcelamento do objeto.

7. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

1. A solução indicada já é a mais alinhada ao ambiente de trabalho do Tribunal.

ANÁLISE DE RISCOS

8. IDENTIFICAÇÃO DOS RISCOS

1. Indicação de código de produto não adequado para os tipos de licenças a serem adquiridas;
2. Dificuldade de adaptação dos usuários ao conjunto de ferramentas online;
3. Aquisição de fornecedor não autorizado pela fabricante.

8.1. IDENTIFICAÇÃO DOS RISCOS DE DEPENDÊNCIA TECNOLÓGICA

1. Dependência de terceiros: Ao utilizar o Office 365, ocorre uma dependência de um provedor de serviços terceirizado para o armazenamento, processamento e proteção dos dados. Isso implica em potenciais riscos relacionados a possíveis falhas no cumprimento de obrigações contratuais, alterações nas políticas de privacidade ou até mesmo encerramento dos serviços.
2.

9. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

9.1. ANÁLISE DOS RISCOS

1. Probabilidade e impacto, ações de prevenção/contingência, responsáveis. Incluídos nas tabelas abaixo.

RISCO 1		Indicação de código de produto não adequado para os tipos de licenças a serem adquiridas;	
Probabilidade (Alta, média ou baixa)		Alta	
	Efeito (Dano)	*Impacto	
1	Possível anulação da licitação	Alto	
2	Fornecimento de um produto não adequado à infraestrutura do Tribunal	Alto	
	Ações de Mitigação e Contingência	Responsável	
1	Consulta de um fornecedor autorizado para o fornecimento da solução	Equipe de Planejamento	

*Impacto (Baixo, Médio ou Alto)

RISCO 2		Dificuldade de adaptação dos usuários ao conjunto de ferramentas online	
Probabilidade (Alta, média ou baixa)		Médio	
	Efeito (Dano)	*Impacto	
1	Rejeição da ferramenta ou subutilização	Médio	
2	Compartilhamento de dados sensíveis por engano	Alto	
3	Compartilhamento de dados de forma inadequada	Médio	
	Ações de Mitigação e Contingência	Responsável	
1	Promoção de treinamentos regulares.	CIS, NSC	

*Impacto (Baixo, Médio ou Alto)

RISCO 3		Aquisição de fornecedor não autorizado pela fabricante.	
Probabilidade (Alta, média ou baixa)		Médio	
	Efeito (Dano)	*Impacto	
1	Problemas na assinatura do contrato	Médio	

2	Problemas na continuidade dos serviços	Alto
3	Rescisão contratual	Médio
	Ações de Mitigação e Contingência	Responsável
1	Exigência de documentação específica para mediação da venda das licenças	Equipe de Planejamento
2	Implantação do Programa de Gestão de Continuidade de Negócios (PGCN)	Assessoria de Gestão Estratégica (AGE)

*Impacto (Baixo, Médio ou Alto)

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

10. RECURSOS MATERIAIS E HUMANOS

- Há necessidade de qualificação do pessoal técnico para lidar com o monitoramento e prevenção de ameaças e vulnerabilidades.
- RECURSOS FORNECIDOS PELO CONTRATANTE
 - Pessoal técnico qualificado para atuação do suporte ao usuário.
 - Pessoal técnico qualificado para atuação na administração e organização das licenças fornecidas, bem como administração dos recursos adquiridos.
 - Recursos de comunicação de dados com capacidade suficiente para suportar as operações.
- RECURSOS FORNECIDOS PELA CONTRATADA
 - Liberação das licenças e recursos associados à cada licença.

11. DESCONTINUIDADE DO FORNECIMENTO

- A descontinuidade do fornecimento deverá ser analisada em fases de ocorrência e duração. No caso de reincidência e/ou ocorrências repetitivas sem a devida justificativa e correspondente aceitação dessa justificativa por parte do Contratante, poderá ser caracterizada a inexecução contratual.
- A instituição do Programa de Gestão de Continuidade de Negócios (PGCN) consta nos itens A054, A055, A056, A057, A058 do Plano de Trabalho de Segurança da Informação e Proteção de Dados, parte do PDTIC 2021-2026. O plano de continuidade é de fundamental importância para o estabelecimento de metas e parâmetros para que a dependência tecnológica seja mitigada.

ANEXO A - LISTA DE POTENCIAIS FORNECEDORES

BRASOFTWARE
INTEGRO CONSULTORES ASSOCIADOS
OFFICER

Detalhes na Informação 0947765.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (PORTARIA DG Nº 129, SEI N. 0930581)

Integrante Demandante: DANILO MAGNO MARCHIORI (substituto: SANDRO MERÇON DA SILVA)

Integrante Técnico: BUENO BORGES DE SOUZA (substituto: LUCAS RIBEIRO CARLIN)

Integrante Administrativo: JOSE ADRIANI BRUNELLI DESTEFFANI (substituto: CARLOS ALBERTO DA ROCHA PADUA FILHO)

Vitória, 09 de maio de 2023.



Documento assinado eletronicamente por **DANILO MAGNO MARCHIORI, Secretário(a)**, em 07/06/2023, às 14:03, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN, Integrante Técnico**, em 07/06/2023, às 14:05, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **JOSE ADRIANI BRUNELLI DESTEFFANI, Secretário(a)**, em 07/06/2023, às 15:48, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **BUENO BORGES DE SOUZA, Integrante Técnico**, em 07/06/2023, às 15:49, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0953182** e o código CRC **80FC9F11**.
