

INST.FED.DE EDUC.,CIENC.E TEC.DO SUL DE MG

Estudo Técnico Preliminar 421/2025

1. Informações Básicas

Número do processo: 23343.005287.2025-45

2. Descrição da necessidade

2.1 Garantir a continuidade e manutenção de licenças em formato digital de solução em programa informático de combate a vírus cibernéticos, vulgo antivírus, que possa ter a competência de detectar, monitorar e combater quaisquer atividades relacionadas a software malicioso que venham ou possam vir a causar danos à equipamento informático do parque técnico da instituição.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia da Informação - Coordenadoria de Suporte de Tecnologia da Informação Everton de Gusmão Rocha	Everton de Gusmão Rocha

4. Necessidades de Negócio

4.1 Solução de software antivírus para garantir a continuidade e manutenção de licenças em formato digital de solução em programa informático de combate a vírus cibernéticos, conhecido como antivírus, que possa ter a competência de detectar, monitorar e combater quaisquer atividades relacionadas a software malicioso que venham ou possam vir a causar danos à equipamento informático do parque técnico da instituição.

5. Necessidades Tecnológicas

5.1 Fundamentalmente a solução deve ser do tipo endpoint, além disso, deverá ser capaz de gerir políticas de segurança distintas, visto que existem demandas personalizadas de acordo com as necessidades de usuários específicos, deve conter funcionalidades essenciais à segurança, como firewall, políticas de acesso a websites, bloqueio de transmissão de informações sensíveis e acesso a informações avançadas sobre as ações executadas, para que assim possam-se realizar auditorias referentes a possíveis danos ao ambiente institucional.

5.2 Deve possuir plataforma para gerência de configurações e ajustes relacionados ao Endpoint. A plataforma deverá possuir características essenciais como envio de relatórios, por e-mail, referentes ao uso das funcionalidades da solução, como websites e aplicações bloqueadas e atividades referentes ao firewall, deverá possuir também dashboard personalizável com as informações que exigem maior atenção, como níveis de ameaça e quantidade de riscos.

5.3 Deverá fornecer atualizações de políticas via rede, fornecer capacidade de agregar múltiplos dispositivos em diferentes unidades organizacionais, garantindo assim maior eficácia ao adotar as medidas personalizáveis de segurança.

5.4 O endpoint deverá ser capaz de analisar as ações tomadas pelo usuário e identificar possíveis incidentes que afetem a rede de computadores. A solução deverá ser capaz de remover outras soluções que ajam de maneira concomitante com a mesma.

5.5 O endpoint também deverá possuir controles relacionados a permissibilidade, para que apenas usuários administradores possam realizar configurações e ajustes manuais, como reiniciar módulos. Deverá realizar varreduras em unidades externas (exemplo: USB) que venham a se conectar com o dispositivo, e, caso possuam arquivos ou possam vir a causar malefícios, tomar medidas para o bloqueio da atividade suspeita.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1 A solução de software antivírus deverá possuir as seguintes funcionalidades:

- Antimalware: a solução deverá realizar análises heurísticas acerca dos tipos de vírus que podem vir a causar malefícios ao dispositivo, tais quais vírus, worms, trojans, spywares, adwares, keyloggers, rootkits, entre outros. Deverá também conter formas personalizáveis de escaneamento envolvendo processamento em nuvem;
- Análise de riscos dos Endpoints: identifica, realiza o acesso e remedia vulnerabilidades através de análises de vulnerabilidade, que por sua vez podem ser agendadas ou requisitadas. Após realizar a análise, a solução deverá fornecer um resumo dos riscos encontrados em uma dashboard, ou um relatório, e instruir dicas de como mitigar as vulnerabilidades;
- Controle avançado de ameaças: destinado a aplicações maliciosas que por ventura venham a evadir a análises heurísticas. Neste módulo, a solução deverá monitorar, de maneira contínua, o comportamento dos processos e bloquear possíveis formas de manipulação;
- Controle avançado contra exploração de vulnerabilidades: a solução deverá atuar contra ataques zero-day. Neste módulo, a solução se atualizará sobre os exploits mais recentes para que possa mitigar vulnerabilidades que possam ter se evadido de outras varreduras. Deverá acompanhar processos e proteger o dispositivo contra brechas de segurança;
- Controle de conteúdo: a solução deverá executar ações como controle de tráfego, controle de acesso a web, proteção de dados e controle de aplicações;
- Controle de dispositivos: prevenir que dados sensíveis ou vírus sejam atrelados ao computador via dispositivos removíveis, como CD/DVDs, pendrives, dispositivos de armazenamento, entre outros;
- Defesa em ataques relacionados a rede: a solução deverá realizar uma análise do tráfego de rede a fim de identificar vulnerabilidades;
- Firewall: este módulo deverá controlar a atividade de rede nas aplicações do computador.
- Detecção e Resposta em Endpoints (EDR): a solução deverá realizar monitoramento contínuo dos endpoints, detectar ameaças avançadas por análise comportamental, permitir investigação forense dos incidentes e possibilitar resposta remota, como isolamento do endpoint, bloqueio de processos e remediação.
- As licenças deverão ser multiplataforma, permitindo a instalação em diferentes sistemas operacionais e dispositivos, sem restrições prévias.

Dos serviços correlacionados

A contratada deverá prestar serviços de manutenção e suporte técnico da solução de software, durante toda a vigência contratual, como segue:

6.2 Manutenção corretiva: correção de defeitos / erros identificados na solução contratada, abrangendo comportamentos inadequados que causem problemas de uso ou funcionamento e quaisquer desvios em relação a requisitos estabelecidos;

6.3 Manutenção Adaptativa: adequação na solução de software contratada, em decorrência de mudanças que não impliquem inserção, alteração ou exclusão de requisitos funcionais;

6.4 Manutenção de Interface: adequação na solução de software contratada para promover mudanças de interface e layout, sem alteração de funcionalidades sob o ponto de vista do usuário;

6.5 Manutenção Evolutiva: mudanças em requisitos funcionais da solução de software já concluído que implicam inclusão, alteração e/ou exclusão de funcionalidades;

6.6 Os serviços de manutenção compreendem não apenas a modificação do código da aplicação, mas também todas as atividades necessárias para o atendimento de quaisquer das manutenções acima;

6.7 Não será admitida cobrança retroativa de valores referentes a serviços correlacionados e de atualização de versões;

6.8 Não será admitida a cobrança de valores para eventual reativação de serviços agregados;

6.9 Não será admitida a cobrança de valores relativos ao serviço de correção de erros, inclusive retroativos, que devem ser corrigidos sem ônus à contratante, durante o prazo de validade técnica da subscrição dos softwares, nos termos do Capítulo III da Lei nº 9.609, de 19 de fevereiro de 1998.

6.10 A contratada obriga-se a manter a solução de software atualizada.

6.11 A contratada obriga-se a disponibilizar todas as atualizações da solução de software, bem como novas funcionalidades incorporadas da solução sem incidência de custos para a contratante.

Do Suporte Técnico

6.12 A contratada deverá disponibilizar plataforma, email e/ou WhatsApp para abertura de chamados de suporte técnico;

6.13 A abertura de chamados deverá permitir aos usuários da contratante registro de qualquer tópico, incluindo tanto dúvidas de uso do sistema quanto a ajustes/solicitações de funcionalidades;

6.14 Os níveis de serviço para atendimento de chamados de suporte técnico deverão observar o que segue:

6.14.1 Solicitação Crítica: relativo a incidentes que impeçam totalmente as atividades da instituição, ou que impeça parcialmente qualquer atividade para os operadores da solução, sendo que tais processos precisam ser executados imediatamente, sem exceder o prazo limite de 48 (quarenta e oito) horas para solução;

6.14.2 Solicitação Urgente: Relativos a incidentes que impeça totalmente as atividades de um operador, sendo que tais processos precisam ser executados em um prazo curto, limitado a 7 (sete) dias para solução;

6.14.3 Solicitação Necessária: Relativos a incidentes que impeçam parcialmente as atividades de um operador ou que reduza a produtividade de um setor, esta solicitação tem um prazo para atendimento mais flexível, limitado a no máximo 15 (quinze) dias para solução;

6.14.4 Solicitação Desejável: Solicitação de melhoria ou nova funcionalidades, devendo ser respondida em até 14 (quatorze) dias, indicando a viabilidade ou não da implementação pela contratada, e se for o caso, apresentar estimativa de prazo para atendimento.

Dos Direitos Autorais

6.15 Esta contratação não inclui a cessão de direitos de propriedades intelectuais e autorais da solução a ser contratada;

6.16 Deverão ser observadas eventual política de privacidade de software;

6.17 É vedado o acesso não autorizado aos códigos-fonte do Software, sob pena de indenização e multa por parte do infrator;

6.18 A contratada é detentora dos direitos autorais sobre o Software, protegidos e regulados pela Lei 9.609/98, ou deter direitos de comercialização;

Da Proteção de Dados

6.19 A base de dados do software decorrente do uso da solução será de propriedade da contratante. Em caso de encerramento contratual, a contratada deverá disponibilizar para a contratante aquela base de dados gerada na execução dos serviços, incluindo documentos e elementos de informação (como dados pessoais dos servidores), em um formato que permita a migração, para que ela tenha condições de migrar as informações para sua base de dados.

6.20 A contratada deverá informar o seu Encarregado pela proteção de Dados, nos termos do art. 41 da Lei Federal nº 13.709/18;

6.21 As partes deverão assinar o Termo de Compromisso de Manutenção de Sigilo conforme modelo que constará do termo de Referência.

6.22 O software deverá seguir as regulamentações de coleta, uso, tratamento e descarte de dados pessoais previstas na Política de Privacidade e Proteção de dados do IFSULDEMINAS (Resolução nº 131/2021/CONSUP/IFSULDEMINAS), assim como a Política de Segurança da Informação do IFSULDEMINAS (Resolução nº 355/2023/CONSUP/IFSULDEMINAS).

7. Estimativa da demanda - quantidade de bens e serviços

7.1 A estimativa de quantitativos para atendimento desta demanda foi feita em função do parque de equipamentos, onde:

- Reitoria: requer 220 subscrições, incremento de 20 subscrições;
- Campus Três Corações: requer 350 subscrições, incremento de 350 subscrições;
- Campus Carmo de Minas: requer 250 subscrições, incremento de 50 unidades.

7.2 Todas as demandas identificadas são maiores do que aquelas do contrato atual, refletindo o aumento do parque tecnológico advindos, principalmente, de ativos empenhados no final de 2025.

7.3 Para atendimento do futuro Campus Itajubá, dado que não se conhece quando a infraestrutura estará disponível, a respectiva demanda será atendida com aditivo ao futuro contrato da Reitoria. Neste momento a demanda está estimada em 100 subscrições (dois laboratórios e o corpo administrativo).

8. Levantamento de soluções

Catálogo de soluções de TIC com condições padronizadas

8.1 A solução para atendimento desta demanda não se encontra disponível no catálogo de soluções de TIC com condições padronizadas, conforme consulta feita ao sítio <https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/catalogos-de-solucoes-de-tic-com-condicoes-padronizadas-para-licenciamento-de-software>, em 22/12/2025, os quais contemplam apenas soluções de softwares comerciais a exemplo do print que segue:

Catálogos Publicados



Necessidades similares em outros órgãos ou entidades da administração pública e as soluções adotadas

8.2 Entendemos que demais órgãos e entidades da administração pública, notadamente da área de ensino, adotam soluções de mercado, como atesta a pesquisa de preços realizada na base de dados do governo federal.

A existência de software público brasileiro

8.3 A solução para atendimento desta demanda não se encontra disponível no portal de software público brasileiro, conforme consulta feita ao sítio https://softwarepublico.gov.br/social/search/software_infos, em 19/11/2026.

As alternativas de mercados

8.4 A necessidade só pode ser atendida com software de antivírus do tipo endpoint pois as demandas referentes às soluções de segurança pretendidas necessitam de frequentes atualizações especializadas, devido ao constante irromper de novos riscos oriundos da rede mundial de computadores.

9. Análise comparativa de soluções

9.1 Atualmente esta necessidade está sendo atendida através do contrato 11/2021, com vigência até 01/05/2026, derivado do processo administrativo 23343.000398.2020-31 que se refere-se Pregão Eletrônico SRP nº 03/2021 - Contratação de empresa especializada na prestação de serviço de subscrição de software antivírus;

9.2 A solução atual utilizada na instituição é o software "FSECURE", durante o período de sua utilização o mesmo comportou-se de maneira satisfatória. No entanto, foi possível verificar que é necessário o acréscimo de nova(s) funcionalidade(s) e, ao menos, a versão não deve ser usada.

9.3 A necessidade só pode ser atendida com software de antivírus do tipo endpoint pois as demandas referentes às soluções de segurança pretendidas necessitam de frequentes atualizações especializadas, devido ao constante irromper de novos riscos oriundos da rede mundial de computadores.

9.4 A terminologia derivada de "software de antivírus endpoint" se refere a solução que atua em conjunto com múltiplas aplicações relacionadas a segurança, visto que, para se atingir um ínfimo de segurança, múltiplos fatores devem ser considerados, contemplando antimalware, análise de riscos dos endpoints, controle avançado de ameaças, controle avançado contra exploração de vulnerabilidades, controle de conteúdo, controle de dispositivos, defesa em ataques relacionados a rede, firewall.

9.5 A solução deve fornecer suas funcionalidades para os sistemas operacionais Microsoft Windows 11, Linux, Android e IOS visto que o mesmo é amplamente utilizado no mercado e nas instalações do parque informático da requisitante do presente estudo técnico preliminar.

9.10 Todavia, há no mercado outras soluções de antivírus endpoint que possam vir a atender as necessidades aqui elencadas, embora, no momento de redação do presente estudo técnico preliminar, nem todas as soluções aqui destacadas puderam atender os requisitos em sua totalidade.

9.11 Podem existir soluções mais completas porém neste documento foram elencadas soluções largamente utilizadas no mercado. Existem soluções que já são utilizadas por outras instituições públicas

9.12 No mercado também existem soluções alternativas, como TrendMicro. Não foram encontradas soluções open source de antivírus endpoint que atendam as necessidades da instituição.

	Armadito-av	BitDefender	ClamAV	WithSecure	Kaspersky	TrendMicro
Antimalware	Não	Sim	Não	Sim	Sim	Sim
Análise de riscos dos Endpoints	Não	Sim	Não	Sim	Sim	Sim
Controle avançado de ameaças	Não	Sim	Não	Sim	Sim	Não

Controle avançado contra de exploração vulnerabilidades	Não	Sim	Não	Sim	Sim	Não
Controle de conteúdo	Não	Sim	Não	Sim	Sim	Sim
Controle de dispositivos	Não	Sim	Não	Sim	Sim	Sim
Defesa em ataques relacionados a rede	Não	Sim	Não	Sim	Sim	Sim
Firewall	Não	Sim	Não	Sim	Sim	Sim
Deteção e Resposta em Endpoints (EDR)	Não	Sim	Não	Sim	Sim	Sim
Multiplataforma	Não	Sim	Não	Sim	Sim	Sim

9.13 Dada a tabela acima, pode-se observar que existem diversas soluções presentes no mercado que possam cumprir, ao menos em partes, os requisitos aqui elencados. Destacam-se a solução Bitdefender e a solução Kaspersky que, em sucinta análise, demonstraram capazes de gerir as necessidades da instituição.

9.13 Além dos aspectos abordados nas análises registradas nos itens anteriores, registra-se a seguir outros relevantes e aqueles previstos na IN SGD ME 94/2022 que devem ser avaliados em uma contratação de TIC.

Aspecto da solução	Solução	Avaliação
Necessidade de ajuste da infraestrutura atual	Soluções de mercado	Apenas instalação
Necessidade de contratação de serviços adicionais correlacionados ao objeto da contratação	Soluções de mercado	Não
Grau de dependência tecnológica	Soluções de mercado	Total
Grau de Integração de serviços e usabilidade ao usuário	Soluções de mercado	Console de gestão amigável
Necessidade de revisão de processos de trabalho para utilização mais eficiente da solução	Soluções de mercado	Não

Maturidade do mercado no fornecimento da solução	Soluções de mercado	Madura
Pontos de falha	Soluções de mercado	Não identificado
Encargos de implantação da solução	Soluções de mercado	Não há
Necessidade de treinamento para o usuário	Soluções de mercado	Sim
Necessidade de treinamento para os gestores da solução	Soluções de mercado	Não se aplica

Aspectos da IN SGD ME 94/2022	Solução	Sim	Não	NA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Soluções de mercado	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Soluções de mercado		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Soluções de mercado		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Soluções de mercado	X ePing		
A Solução é aderente às regulamentações da ICPBrasil?	Soluções de mercado			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Soluções de mercado			X

Conclusão

9.14 Contratação de solução de mercado de acordo com os requisitos mínimos elencados neste estudo técnico.

10. Registro de soluções consideradas inviáveis

10.1 De acordo com a primeira tabela do item 9, as seguintes demandas são inviáveis:

10.1.1 Armadito-av;

10.1.2 ClamAV;

10.1.3 TrendMicro

10.2 No mais dev-se manter o seguintes registro feito em 2021 quanto à solução McAfee, no sentido de se verificar eventual evolução:

10.2.1 O uso da solução de segurança da McAfee na instituição tornou-se moroso em decorrência ao alto número de falsos positivos, complexidade da manutenibilidade e provimento da solução aos endpoints, gerência dos pacotes de instalação, políticas de uso e do processo de desinstalação, o qual causou transtornos imensuráveis aos usuários e a equipe técnica;

10.2.2 O termo “falsos positivos” é caracterizado por situação onde a solução de proteção identifica, indevidamente, um ato de ataque ou atitude maliciosa sendo que o mesmo não é real.

11. Análise comparativa de custos (TCO)

Do custo total estimado da contratação

11.1 Para estimativa do custo total de contratação foram realizadas pesquisa de preços nos termos dos incisos I e IV do artigo quinto da Instrução Normativa SEGES 65/2021 e conforme dados da tabela a seguir.

11.2 Considerando a abrangência do CATSER 27502 (Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software), que por sua natureza genérica suporta uma vasta gama de serviços de subscrição de software, verificou-se que a consulta direta ao sistema de 'Pesquisa de Preços' do Governo Federal resulta em um volume excessivo de dados heterogêneos. Isso ocorre devido a falta de filtro quanto ao objeto contratado.

11.3 Diante da inviabilidade operacional de realizar uma análise individualizada de cada um dos inúmeros processos listados naquele sistema, optou-se pela metodologia de pesquisa direta em contratações similares de outros órgãos.

11.4 Essa abordagem permite uma comparação mais fidedigna, garantindo a consistência do preço de referência.

11.5 Para fins de comparabilidade, foi adotado como parâmetro o valor unitário mensal dos contratos, mitigando as distorções causadas pelas diferentes metodologias utilizadas na contratação pelos órgãos. Os valores obtidos são conforme tabela a seguir.

11.6 Não foi realizada pesquisa de preços de mercado.

11.7 Nos preços registrados na tabela a seguir está evidenciada uma disparidade entre os processos analisados, não tendo sido determinante para aqueles preços a quantidade contratada.

11.8 Sendo assim, opta-se por extrair o valor médio unitário estimado para a contratação considerando apenas os processos Centro Logístico do Material da Marinha da Câmara Municipal de Betim - MG que é de 56,88 anual ou 4,74 mensal, tendo em consideração o valor pago no contrato ainda vigente (veja a análise comparativa de custo).

Órgão	Qtd.	Vigência	Valor Total da Contratação	Valor por licença Ano	Valor por licença Mês
389047 - CONSELHO FEDERAL DOS REPRESENTANTES COMERCIAIS	886	36 meses	R\$ 369.462,00	R\$ 139,00	R\$ 11,58
740014 - CENTRO LOGISTICO DO MATERIAL DA MARINHA	40.000	12 meses	R\$ 2.844.000,00	R\$ 71,10	R\$ 5,93
090028 - TRIBUNAL REGIONAL FEDERAL DA 2A. REGIAO	8.000	60 meses	R\$ 1.832.000,00	R\$ 229,00	R\$ 19,08
925814 - TRIBUNAL DE JUSTIÇA DO ESTADO DE TOCANTINS	4.000	36 meses	R\$ 860.000,00	R\$ 215,00	R\$ 17,92
CÂMARA MUNICIPAL DE BETIM/MG - CMB	300	36 meses	R\$ 38.304,00	R\$ 42,56	R\$ 3,55

11.9 Desta forma, o valor estimado para a contratação é conforme dados da tabela a seguir:

Item	Descrição (A)	Quant.	Fonte	R\$ unitário mensal para 850 licenças	R\$ total para 1 ano	R\$ total para 2 anos
01	Subscrição de 820 licenças de software antivírus	24 meses	Governo	3.886,80	46.641,60	93.283,20
Valor médio estimado						

Análise comparativa de custos

11.10 Para efeitos de análise comparativa de custos utilizaremos o valor estimado para esta contratação e aquele do último aditivo da solução corrente, tendo em vista que a pesquisa de preços na base de dados do governo contempla mais de uma solução de antivírus:

11.10.1 Custo unitário anual estimado: 3.886,80;

11.10.2 Custo unitário anual corrente: 1.643,35;

11.10.3 Custo unitário anual estimado é 2,3652 maior do que o corrente;

11.10.4 Apesar dessa diferença significativa, tem-se que considerar que em relação ao contrato atual está-se adicionando dois requisitos importantes para tornar a solução a ser contratada mais robusta e alinhada à necessidade da Instituição;

11.10.5 Entende-se que a ausência desses requisitos na contratação atual, de 2021, foi determinante na obtenção do custo correspondente, mas a análise técnica atual determinou que a exigência de dois novos requisitos são fundamentais para obtenção de solução mais robustas, considerando que neste tempo os ataques cibernéticos também evoluíram.

Cálculo do custo total de propriedade - TCO

11.11 Para efeitos do custo total de propriedade estimado pode-se considerar a vigência máxima de 10 anos conforme estabelecido pela Lei 14.133/2021, resultando em R\$466.416,00.

Da necessidade de submissão ao SISP

10.12 Deve-se adotar estratégia de apenas permitir adesão dos Campi da Instituição, para que não se tenha que submeter o processo de contratação ao SISP, pois se tivermos que observar o rito da INSTRUÇÃO NORMATIVA SGD/MGI Nº 6, DE 29 DE MARÇO DE 2023 não terá a nova contratação em tempo.

Do parcelamento

10.13 A adjudicação de proposta deverá se dar por unidade da Instituição (Reitoria e cada um dos campi).

12. Descrição da solução de TIC a ser contratada

12.1 Eventual contratação, através de pregão registro de preços, de empresa especializada para fornecimento de subscrições de licenças de software antivírus, para atendimento de demandas de segurança da informação das unidades da Instituição.

13. Estimativa de custo total da contratação

Valor (R\$): 93.283,20

13.1 R\$93.283,20 (noventa e três mil, duzentos e oitenta três reais e vinte centavos) para vigência contratual de 2 anos.

14. Justificativa técnica da escolha da solução

14.1 A solução demandada é tecnicamente viável tendo em vista a experiência acumulada, desde 2021, através do contrato de prestação do serviço atual. No mais, a solução a ser contratada classificada como serviço comum, de natureza continuada, cujas especificações podem ser objetivamente definidos de acordo com padrões de mercado.

15. Justificativa econômica da escolha da solução

15.1 A solução demandada também é economicamente viável, tendo em vista que a estimativa do valor da contratação, custo máximo, está de acordo com a Instrução Normativa SEGES 65/2021.

16. Benefícios a serem alcançados com a contratação

16.1 Com a contratação de subscrição de licenças de software antivírus pretende-se atingir os objetivos abaixo:

16.1.2 Garantir maior segurança na utilização de soluções digitais, equipamentos informáticos, bem como aos usuários da instituição;

16.1.2 Monitorar atividades maliciosas de possíveis equipamentos comprometidos;

16.1.3 Definir políticas de proteção específicas de acordo com as demandas;

16.1.4 Obter informações avançadas para auditar possíveis atividades suspeitas e possíveis danos ao parque informático.

17. Providências a serem Adotadas

17.1 Encaminhar, em tempo, os artefatos do planejamento de contratação para o setor reponsáveis pelos processos de licitações.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1 Declara-se a viabilidade da contratação visto que:

18.1.1 O objeto desta demanda enquadra-se como serviço comum por possuir padrões de desempenho e características gerais e especificações usualmente encontradas no mercado;

18.1.2 Há mais de uma solução disponível no mercado que atendem aos requisitos estabelecidos, o que proporcionará concorrência;

18.1.3 Esta contratação está prevista no Plano Diretor de TIC 2024 - 2026, assim como no Plano Anual de Compras 2026;

18.1.4 Os requisitos desta demanda estão de acordo com o Anexo - I DIRETRIZES ESPECÍFICAS DE PLANEJAMENTO DA CONTRATAÇÃO - CONTRATAÇÃO DE LICENCIAMENTO DE SOFTWARE E SERVIÇOS AGREGADOS da Instrução Normativa SGD/ME 94/2022.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

JAIME DONIZETE BONAMICHI

Equipe de apoio



Assinou eletronicamente em 30/12/2025 às 08:46:09.

VERA CAROLINA DA SILVA

Equipe de apoio



Assinou eletronicamente em 30/12/2025 às 08:53:17.

EVERTON DE GUSMAO ROCHA

Equipe de apoio



Assinou eletronicamente em 30/12/2025 às 09:23:35.