



---

ANEXO II  
ESPECIFICAÇÕES TÉCNICAS OBRIGATÓRIAS

---

O serviço de sistemas de software integrados para a gestão pública nas áreas administrativa, financeira e fiscal para a PMMC-MG deverá atender aos seguintes requisitos técnicos, sob pena de desclassificação:

1. Garantir o perfeito funcionamento dos sistemas e seus respectivos módulos durante toda a vigência do contrato, não sendo permitido o uso de senhas, licenças ou travas periódicas que impeçam o bom funcionamento das funcionalidades desses sistemas.
2. Conter um Sistema Gerenciador de Banco de Dados (SGBD) Relacional, com controle transacional e com recursos para garantir a integridade e a recuperação dos dados por meio das ferramentas de "*backup*" e "*recovery*".
3. Possuir suporte à integração com LDAP, Active Directory e realizar a busca dinâmica de usuários na base de dados.
4. Possibilitar ao administrador do sistema vincular a um determinado usuário (novo ou já existente) a entrada no sistema utilizando o acesso correspondente ao Active Directory. A solução deve impedir o acesso de usuários com *status* bloqueado no Active Directory.
5. O sistema deverá impedir o acesso de usuários cujo vínculo funcional no sistema de Recursos Humanos indique afastamento, férias ou desligamento.
6. O sistema deverá estar em acordo com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).
7. De acordo com o princípio da economicidade e eficiência, o sistema contratado deverá utilizar um único SGBD com licença *open source*. Será aceitável um SGBD com licença paga, desde que a CONTRATADA se responsabilize por oferecer licenças originais sem qualquer ônus ou prazo para cessão à CONTRATANTE. Não será admitido SGBD sem garantia de assistência técnica.
8. Em caso de queda de energia ou falha de *softwares* ou *hardwares*, os sistemas deverão possuir ferramentas e dispositivos para manter a integridade dos dados, contendo mecanismos de proteção que impeçam a perda de transações já efetuadas, possibilitando deste modo, a segurança total dos dados e mantendo a integridade do Banco de Dados.
9. O sistema deverá permitir *backups* do banco de dados, com possibilidade de alteração da periodicidade e dos usuários que podem realizá-los, os quais deverão receber permissão especial para tanto. A administração dessas permissões deverá ser feita em nível de banco de dados, com ferramentas nativas do SGBD. Deverá possibilitar ainda, *backups* do tipo incremental (somente das alterações executadas).
10. O sistema deverá permitir o monitoramento das rotinas em execução sobre o banco de dados que poderão ser realizadas com ferramentas nativas do SGBD.
11. Em acordo com o princípio da economicidade, o sistema deverá ser homologado para o Sistema Operacional *Microsoft Windows Server* 2012 R2, 2016 e 2019 ou superior nos servidores, Banco de Dados *Microsoft SQL Server* e nas estações de trabalho o *Windows* 7, 8, 10 e 11, padrão tecnológico da Prefeitura Municipal de Montes Claros. A CONTRATADA poderá implantar o sistema ofertado em padrão tecnológico diferente do adotado atualmente pela PMMC-MG, desde que se responsabilize pelos custos de aquisição das licenças dos *softwares* necessários, bem como a instalação e configuração para o correto funcionamento do sistema contratado.
12. Possibilitar que os aplicativos sejam acessados por usuários remotos, utilizando a Internet



como meio de conexão.

13. O sistema poderá ser acessado por diversos usuários ao mesmo tempo, caracterizando um sistema multiusuário.
14. Possibilitar o registro de usuários e a definição de suas permissões de acessos individualizáveis em nível de programa. Dentre as permissões de acesso devem constar poderes para incluir, alterar, consultar e excluir dados. Ao usuário deverão ser exibidas somente as informações e opções do sistema às quais possua autorização de acesso em conformidade com a Lei Geral de Proteção de Dados (LGPD). O cadastro do usuário deverá manter os seguintes atributos mínimos:
  - 14.1. Identificador único do usuário (*login*).
  - 14.2. Dados pessoais (nome completo, CPF e número de matrícula);
  - 14.3. Dados de contato (e-mail, celular, ramal de trabalho).
  - 14.4. Unidade administrativa à qual está vinculado.
  - 14.5. Senha de autenticação para acesso ao sistema.
  - 14.6. Indicativo de bloqueio da conta de usuário através de um atributo ou período de validade para as contas de usuário cadastradas no sistema.
  - 14.7. Possuir funcionalidade que permita a criação e o gerenciamento (consulta, alteração e exclusão) de grupos de usuários mantendo, para cada grupo, os seguintes atributos:
    - 14.7.1. Nome do grupo.
    - 14.7.2. Descrição.
  - 14.8. Relação de usuários que o compõe.
15. Os procedimentos de definição de usuários e senhas utilizados pelo sistema devem ser executados pela CONTRATANTE, sob orientação da CONTRATADA. 19. Deverão ser registrados os acessos - entradas (*login*) e saídas (*logoff*) - dos sistemas em um registro de log, de modo que sejam gravadas as seguintes informações: data, hora e usuário.
16. O Sistema deverá possuir gravações de *logs* e trilhas de auditoria com registro das operações realizadas pelos usuários no sistema, bem como, módulo de auditoria com possibilidade de consultas e relatórios dos registros dos *log* e trilhas para os usuários que tenham perfis associados à função de auditoria. Essa rotina deverá possibilitar a realização de consultas nas operações realizadas pelos diversos usuários, informando no mínimo quem realizou determinadas operações, o que foi realizado, quando foi realizada (mínimo: data, hora, minuto e segundo) a operação e onde foi realizada a operação (mínimo: endereço lógico).
17. A consistência dos dados de entrada, tais como validade de datas, de dígitos verificadores e de campos com preenchimento obrigatório, deverá ser realizada campo a campo, tanto no momento da entrada quanto na gravação dos dados, de forma a garantir a integridade referencial, consistência, atualidade e inviolabilidade dos dados feita entre as diversas tabelas dos aplicativos através do próprio aplicativo.
18. Os relatórios apresentados deverão estar no formato gráfico, para serem impressos em impressoras laser e jato de tinta, e ainda possibilitar a(o):
  - 18.1. visualização dos relatórios em tela.
  - 18.2. ampliação (*zoom*) dos relatórios emitidos em tela.
  - 18.3. inserção de informações adicionais no cabeçalho e rodapé do relatório, demonstrando: usuário, data/hora de emissão, comentários adicionais, e seleção utilizada para a emissão.
  - 18.4. Salvamento de relatórios em formato “.pdf”, “.txt”, “.csv”, “.html” e “.xls”. 22.5. integração com correio eletrônico para possibilitar o envio e recebimento de mensagens e arquivos de modo automático.



- 18.5.** Utilizar a língua portuguesa (Brasil) para toda e qualquer comunicação dos sistemas aplicativos com os usuários.
- 19.** Permitir que o usuário desista a qualquer momento da operação corrente. **25.** Possuir ajuda *online* para orientar o usuário a utilizar o sistema. Este auxílio deve ser no idioma Português, com fácil leitura e entendimento.
- 20.** Na hipótese da solução utilizar a arquitetura cliente-servidor, deve-se possibilitar o controle automático da integridade quanto à compatibilidade das versões dos artefatos distribuídos e implantados nas camadas que compõem o sistema.
- 21.** Na hipótese da solução utilizar a arquitetura cliente-servidor, o sistema deve possibilitar que os programas executáveis sejam instalados nas estações clientes, provendo rotinas de atualização automática desses programas a partir do servidor, especialmente no caso de substituição de versões.
- 22.** Possuir total aderência à legislação Federal e do Estado de Minas Gerais e do Município de Montes Claros-MG, deste modo, é exigido do fornecedor ter compromisso à imediata adequação dos sistemas no caso de possíveis alterações das normas.
- 23.** Os módulos do sistema deverão gerar arquivos de intercâmbio de dados para alimentar os sistemas de Auditoria do TCE-MG e de quaisquer outros órgãos das esferas estaduais e federais, conforme os parâmetros determinados por estes, e de acordo com seus layouts, e deverão estar em conformidade e atender o Plano de Contas Aplicado ao Setor Público (PCASP), segundo as Normas Brasileiras de Contabilidade Aplicadas ao Setor Público (NBCASP) e o Manual de Contabilidade Aplicada ao Setor Público (MCASP), Sistema de Informações sobre Orçamentos Públicos em Educação (SIOPE), Sistema de Informações sobre Orçamentos Públicos em Saúde (SIOPS), eSocial, EFD-Reinf, DCTFWeb e demais sistemas de prestação de contas, obrigações acessórias, auditoria e fiscalização instituídos ou que venham a ser instituídos durante a vigência contratual, mantendo-se permanentemente atualizados em decorrência de alterações legais, normativas ou tecnológicas, sem qualquer ônus adicional para a CONTRATANTE.
- 24.** Os sistemas deverão atender à Lei Complementar nº 131/09 (Lei da Transparência), com a geração automática dos dados para o Portal da Transparência, gerando os dados sem intervenção manual por parte dos usuários dos sistemas.
- 25.** Os sistemas deverão atender e garantir o disposto no Decreto Federal nº 10.540/2020 sobre o SIAFIC – Sistema Único e Integrado de Execução Orçamentária, Administração Financeira e Controle ou decretos que possam sucedê-lo.
- 26.** Disponibilizar funcionalidade para gestão das emendas parlamentares, em conformidade com a INSTRUÇÃO NORMATIVA TCE-MG N. 05/2025 e demais legislações vigentes, contemplando o cadastro, acompanhamento, execução, controle, prestação de contas, emissão de relatórios e integração com os módulos Contábil, Tesouraria e Portal da Transparência.
- 27.** O sistema Integrado de Gestão Pública deve possuir integração nativa entre os seus módulos, visando a agilização dos fluxos e dos processos internos, evitando retrabalho, redundâncias e distorções. Possuir documentação completa, clara, inteligível e organizada para instalação e uso do *software*.
- 28.** A empresa CONTRATADA deverá disponibilizar a documentação do sistema e dos módulos contratados relativos aos modelos Entidade x Relacionamento e Dicionário de Dados.
- 29.** O sistema deverá disponibilizar ferramentas proprietárias ou de acesso livre que permitam aos usuários finais montarem relatórios por meio da seleção de campos nas tabelas existentes, para customização e montagem de relatórios sintéticos e analíticos, possibilitando:
- 29.1.** Definição de *layout*.



- 29.2. Inclusão (integração) de qualquer campo das tabelas existentes.
- 29.3. Agrupamento por classes.
- 29.4. Totalização dos campos e classes.
- 29.5. Ordenação numérica, alfabética e/ou por período, de qualquer campo ou classe, quando possível.
- 30. O provedor de nuvem deverá possuir no mínimo (2) dois datacenters, em localidades diferentes, e possibilitar escolha do local de residência dos dados com o intuito de otimizar performance e taxas de transmissão
- 31. O provedor de nuvem deve ser autosuficiente e garantir a entrega dos serviços em alto padrão. Para isso, deve atender as seguintes certificações e creditações de segurança e conformidade internacionais ou documentação equivalente: ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 22301, ISO 9001, SOC 1, SOC 2 e SOC 3. Qualquer documento ou referência de acesso público deverá ser apresentado em nome do provedor através de fontes públicas como relatórios ou websites, sendo facultado ao CONTRATANTE promover diligência destinada a esclarecer ou complementar informações.
- 32. Todos os produtos fornecidos pela Contratante, devem ser acessíveis através de https, ou seja, devem suportar o protocolo seguro SSL.
- 33. O provedor de nuvem deverá oferecer, um serviço de banco de dados relacional que possibilite cópias de segurança e snapshots de qualquer tamanho de uma região de nuvem para outra com o objetivo de facilitar o disaster recovery.
- 34. O provedor de nuvem deverá disponibilizar dashboard de acesso para criação, inativação e reset de senha dos usuários.
- 35. A escalabilidade da aplicação no ambiente de nuvem deve ser capaz de ajustar os recursos conforme a demanda de usuários conectados, garantindo que o desempenho e a produtividade não sejam comprometidos. Dessa forma, a infraestrutura se adapta às necessidades, oferecendo flexibilidade e alta disponibilidade para manter a produtividade em níveis ideais.
- 36. O provedor de nuvem deverá suportar resizing de máquinas virtuais (memória, discos, processador), proporcionando um dimensionamento rápido e instantâneo (média de 5 min) sempre que necessitar e sem necessitar intervenção física no equipamento.
- 37. A contratada deverá disponibilizar controle e monitoramento de segurança 24x7x365 em todo seu ambiente cloud, por meio de estrutura de Centro de Operações de Segurança (Security Operations Center), contemplando: Gerenciamento e Correlação de Eventos de Segurança (Security Information and Event Management), Monitoramento de Segurança e Detecção de Ameaças (Security Monitoring and Threat Detection), Inteligência e Avaliação de Ameaças (Threat Intelligence and Threat Assessment), Caça a Ameaças (Threat Hunting), Resposta a Incidentes de Segurança (Security Incident Response), XDR para resposta automática, Threat Intel com análise via IA e análise de Vulnerabilidade.
- 38. A contratada deverá dispor de monitoramento e gestão de eventos dos ativos de toda sua estrutura cloud, em modelo 24x7x365, executado remotamente por meio de NOC (Network Operations Center), identificando de forma proativa, incidentes e problemas nos ativos de rede, sistemas e serviços por meio de verificação de logs, parâmetros de utilização, alarmes na ferramenta de monitoramento e demais informações úteis para minimizar a duração e o impacto do incidente.
- 39. O serviço cloud deverá possuir solução centralizada de segurança do tipo endpoint protection, para todos os recursos acessíveis via protocolos de internet. Deverá ser possível detectar e bloquear ataques zero-day, proteção ativa contra malwares em arquivos e aplicações (em execução ou não) proteção a nível de rede e web com uso integrado de firewall, remoção automática de ameaças, contenção automatizada de dispositivos e aprendizado por IA.



40. A contratada deverá utilizar em sua cloud firewall profissional de rede e web (WAF), bloqueando ataques DDOS, ataques de bots maliciosos, detecção de anomalias, detecção e proteção de API, mitigação e análise avançada de ameaças, trabalho integrado com SOC/SIEM para criação de regras automatizadas.
41. Conformidade com a Lei nº 13.709/2018 (LGPD): os dados deverão ser armazenados preferencialmente em território nacional; havendo transferência internacional, a CONTRATADA deverá comprovar o atendimento aos arts. 33 a 36 da LGPD, atuando como operadora mediante instrumento contratual de tratamento de dados, com obrigação de notificação de incidentes de segurança em até 24 (vinte e quatro) horas do conhecimento.
42. Disponibilizar ambiente de homologação/treinamento apartado do ambiente de produção, com dados anonimizados ou mascarados, disponível durante toda a vigência contratual.
43. O provedor de nuvem deverá fornecer backup diário ao CONTRATANTE e reter esse backup, por pelo menos 30 dias.
44. A CONTRATADA deverá disponibilizar ao Município usuários próprios para acesso às aplicações e aos recursos de acompanhamento dos serviços contratados, com os níveis de permissão necessários à utilização, consulta e fiscalização dos serviços, observadas as políticas de segurança e segregação de responsabilidades da CONTRATADA. O acesso aos componentes de infraestrutura e à administração da plataforma de nuvem permanecerá sob responsabilidade da CONTRATADA. Esse usuário deverá:
  - 44.1. Ser de titularidade exclusiva do Município, com credenciais próprias (login e senha, com suporte a autenticação multifator), não podendo depender de usuário, sessão ou credencial da CONTRATADA para ser acessado ou recuperado;
  - 44.2. A CONTRATADA deverá disponibilizar ao Município, mediante solicitação formal e observados os prazos definidos nos níveis de serviço (SLA), relatórios ou registros de auditoria referentes a acessos, configurações relevantes e desempenho dos serviços contratados, no que for pertinente ao acompanhamento da execução contratual;
  - 44.3. Ser mantido ativo durante toda a vigência contratual e ser o meio formal de transferência de acesso e de dados ao final do contrato ou em caso de transição contratual, de modo a assegurar a portabilidade e a continuidade da prestação do serviço público, vedada qualquer forma de bloqueio, retenção de acesso ou dependência técnica da CONTRATADA;
  - 44.4. A CONTRATADA deverá disponibilizar esses usuários no prazo máximo de 15 (quinze) dias corridos, contados do envio da ordem de serviço, sob pena de aplicação das penalidades previstas neste Termo de Referência para o descumprimento de prazos de implantação, correspondente ao Nível 1 do SLA definido no item 8.52.