SECRETARIA MUNICIPAL DE PLANEJAMENTO E GESTÃO
COMISSÃO ESPECIAL DE LICITAÇÕES DE FINANCIAMENTOS - DLC/SMPG
DOCUMENTO

RESPOSTAS AO PEDIDO DE ESCLARECIMENTOS RECEBIDO EM 14/11/2025:

A Comissão Especial de Licitação (CEL), responsável pela condução da fase externa das licitações dos contratos de financiamento internacionais da Administração Direta e Indireta do Município, à exceção do Departamento Municipal de Água e Esgotos (DMAE), torna públicas as respostas ao pedido de esclarecimentos formulado em 11 de novembro de 2025, após o recebimento da Informação 36792151 que consolidou os subsídios de caráter técnico prestados pelos responsáveis pela elaboração do termo de referência e seus anexos:

1. Treinamento - Divergência entre quantitativos (UST) e descrição detalhada

No item 1.1.3, o treinamento está mensurado em 7 UST. Entretanto, o item 4.2.1 estabelece parâmetros objetivos:

- *2 turmas*
- *até 30 participantes*
- *20 horas-aula cada*
- *formato remoto*
- *conteúdo definido*

Esse escopo fechado não se alinha à métrica UST, usualmente aplicada a serviços sob demanda e não a capacitações com carga horária fixa. Solicitamos confirmar o entendimento que: a) o treinamento será prestado conforme os parâmetros do item 4.2.1; e b) se permanece a mensuração por UST, qual é a metodologia esperada para composição e cálculo da proposta para este item. Para fins de padronização da apresentação das propostas, sugerimos esclarecer se o treinamento deve ter valor fixo por turma/hora ou se a métrica UST deverá ser mantida.

Resposta ao fornecedor:

a) O treinamento será prestado conforme os parâmetros estabelecidos no item 4.2.1 do Termo de Referência, com a realização de 2 (duas) turmas, cada uma com 20 (vinte) horas-aula, em formato remoto e com conteúdo previamente definido;

b) Para fins de padronização das propostas e isonomia entre os licitantes, o treinamento será remunerado por turma, e não pela métrica UST indicada no item 1.1.3. Assim, cada licitante deverá apresentar valor unitário por turma, contemplando toda a carga horária, instrutor, materiais e demais elementos necessários. O item 1.1.3 será ajustado para harmonização terminológica, mantendo-se como referência válida a estrutura definida no item 4.2.1.

2. Operação Assistida - Divergências sobre duração e modalidade

Identificamos divergência entre:

- *Item 1.1.3.5, que prevê até 2 meses presenciais, e*
- *Itens 4.2.5.1 e .4.2.5.2, que preveem 3 meses, sendo:*
    - *1º mês presencial*

- *2º e 3º meses remotos*

Solicitamos confirmar: a) qual é a duração total da operação assistida (2 ou 3 meses); b) se todo o período será presencial ou se seguirá o modelo híbrido descrito nos itens 4.2.5.1 e 4.2.5.2. Tal esclarecimento é essencial para definição de custos de equipe, alocação presencial e composição da proposta global.

Resposta ao fornecedor:

a) A duração total da operação assistida é de 3 (três) meses, conforme estabelecido nos itens 4.2.5.1 e 4.2.5.2 do Termo de Referência.

b) O período seguirá o modelo híbrido previsto nesses itens: 1º mês presencial e 2º e 3º meses remotos. O item 1.1.3.5 será ajustado apenas para harmonização terminológica, mantendo-se como referência válida a estrutura definida no item 4.2.5.

3. Nota: "Valor considerando a disponibilização de 8 horas/dia do profissional"

A nota ao final da tabela de quantitativos (item 1.1.3) indica que o valor considera a disponibilização de 8 horas/dia do profissional, mas não especifica para quais itens a regra se aplica.

Solicitamos esclarecer: a) a quais itens essa jornada de 8 horas/dia se refere; b) se se trata de parâmetro exclusivo para itens mensurados em UST; c) se possui impacto na forma de mensuração ou apenas na composição de custos.

Resposta ao fornecedor:

a) A jornada de 8 horas/dia refere-se aos itens do quadro do item 1.1.3 que envolvem dedicação de profissionais. Essa informação foi inserida com o objetivo de orientar a composição dos custos pelas licitantes.

b) A administração esclarece que a intenção original era definir formalmente que 1 UST corresponde a 8 (oito) horas de trabalho técnico, como forma de padronizar a mensuração e a formação de preços. Contudo, essa equivalência não foi explicitada na redação publicada e será devidamente formalizada na retificação, sem alteração do escopo ou dos quantitativos originalmente previstos.

c) A indicação de 8 horas/dia impacta apenas a composição de custos, enquanto a equivalência “1 UST = 8 horas” será formalmente registrada mediante retificação do item 1.1.3, garantindo clareza, isonomia e alinhamento ao critério inicialmente previsto.

4. Tabela de Quantitativos x Cronograma de Pagamento

Observamos que:

- *A tabela 1.1.3 prevê licença de Uso da Solução (12 meses),*
- *Mas o cronograma de execução (item 4.4.1) não relaciona o pagamento da licença,*
- *Enquanto o item de operação assistida aparece explicitamente no cronograma.*

Além disso, o regime de execução é empreitada por preço global, mas os itens possuem natureza distinta (subscrição mensal x serviços pontuais).
Solicitamos confirmar: a) se o pagamento da licença ocorrerá mensalmente, em parcela única ou atrelado aos marcos do cronograma; b) como se dará o desembolso para os demais itens: conforme quantidades executadas, percentuais do cronograma ou outra metodologia; c) se haverá planilha de formação de preços ou modelo obrigatório de apresentação dos valores de cada item.

Resposta ao fornecedor:

a) O pagamento da licença de uso da solução ocorrerá mensalmente, de forma proporcional ao período contratado. O item correspondente será ajustado no Termo de Referência para harmonização com o cronograma de execução.

b) Os demais itens serão remunerados conforme a entrega de cada serviço, tais como configuração, migração, operação assistida e treinamento. A forma de desembolso será explicitada nos ajustes do item 1.1.3 e no cronograma, garantindo alinhamento entre quantitativos e etapas de execução. A Licença de Uso da Solução permanecerá com pagamento mensal.

c) A planilha constante na Seção 3 do Edital é o modelo de proposta a ser utilizado pelas licitantes. Contudo, considerando a necessidade de harmonização com os quantitativos e com a metodologia de pagamento definida no Termo de Referência, a planilha será ajustada na retificação do edital. A versão retificada será de preenchimento obrigatório, devendo conter os valores unitários de cada item e o valor global da proposta.

5. Ambientes (produção e homologação)

"(Ref.: Termo de Referência, itens 1.1.3.1 e 1.1.3.5, e item 3.5 sobre hospedagem em nuvem)

Considerando que a solução será fornecida na modalidade SaaS (Software as a Service), na qual a aplicação é única e compartilhada entre diversos clientes e usuários, solicitamos confirmar se é realmente necessária a disponibilização de um ambiente de homologação exclusivo (dedicado) para a Prefeitura. No modelo SaaS, todos os testes funcionais, de regressão, segurança e performance são realizados internamente pelo fornecedor, em ambientes controlados e automatizados, antes de qualquer liberação de versão. Esses testes abrangem múltiplos cenários de uso e combinações de configuração, o que garante que cada atualização atenda à diversidade de contextos esperados — algo que um único cliente, isoladamente, não teria condições de reproduzir ou validar de forma completa . Solicitamos confirmar o entendimento de que: A exigência de um ambiente de homologação exclusivo não se aplica ao modelo SaaS multicliente, sendo suficiente o processo de homologação centralizado e documentado pelo fornecedor, com evidências de testes e comunicados prévios de atualização, conforme as melhores práticas ITIL e ISO/IEC 20000."

Resposta ao fornecedor:

A DGTI/SMPG reconhece as particularidades do modelo SaaS multicliente quanto à homologação centralizada. Entretanto, para atender aos requisitos de governança e gestão de riscos:

a) O fornecedor deve apresentar evidências documentadas de seu processo de homologação interna, incluindo testes funcionais, de regressão, segurança e performance, conforme melhores práticas ITIL e ISO/IEC 20000.

b) Disponibilização de canal de informações prévias de atualização devem incluir: release notes detalhadas, impactos esperados, janela de manutenção e plano de rollback.

6. Restore sob demanda e cópia do banco na infraestrutura da Prefeitura

"(Ref.: Termo de Referência, item 3.3.5 e Apêndice A – requisitos de backup e alta disponibilidade)

O item prevê a possibilidade de restauração sob demanda e cópia do banco de dados para a infraestrutura local da PROCEMPA . Solicitamos confirmar o entendimento de que: Tal possibilidade não é aplicável a soluções SaaS multicliente, considerando que nesses modelos, os backups e restores são centralizados, garantindo rastreabilidade e segurança, mas sem permitir cópias físicas da base completa, por conter dados de outros clientes."

Resposta ao fornecedor:

A DGTI/SMPG esclarece que a exigência refere-se exclusivamente aos dados municipais, não à base completa multicliente. Desta forma:

a) O fornecedor deve garantir capacidade de restore segregado, restaurando apenas os dados da PMPA mediante solicitação formal.

b) O restore deve ser realizado em formato recuperável e íntegro.

c) A PMPA deve ter capacidade de exportar seus dados completos a qualquer momento através de mecanismo automatizado, em formatos estruturados e interoperáveis.

d) O fornecedor deve realizar e documentar testes periódicos de disaster recovery (DR), com relatórios de evidência disponibilizados à PMPA, demonstrando a capacidade efetiva de recuperação dos dados municipais.

7. Backup local e ambiente dedicado

"(Ref.: Termo de Referência, item 3.3.5 e 4.5.4 – tutela e segurança da informação)

Solicitamos confirmar o entendimento de que:

Considerando se tratar de contratação na modalidade SAAS, a cópia física do banco poderá ser substituído por acesso controlado a relatórios e exportações estruturadas de dados em formato aberto (ex.: CSV, JSON, XML), conforme os princípios de interoperabilidade e portabilidade previstos na LGPD .

Esse modelo assegura a soberania da Administração sobre seus dados, mantendo a segurança e a segregação lógica sem necessidade de ambiente dedicado."

Resposta ao fornecedor:

A DGTI/SMPG aceita a substituição de cópia física do banco de dados por exportação estruturada, DESDE QUE atendidas as seguintes condições técnicas obrigatórias:

a) Formatos de exportação em padrões abertos e interoperáveis: CSV, JSON, XML ou formatos equivalentes amplamente suportados.

b) Fornecimento obrigatório de dicionário de dados completo, incluindo: estrutura de campos, tipos de dados, relacionamentos, chaves, metadados e mapeamento de dependências.

c) Exportações devem preservar integridade referencial e incluir todos os relacionamentos entre entidades, permitindo reconstrução completa da base de dados em outro sistema.

d) Documentação técnica do processo de exportação e formato dos arquivos gerados, facilitando importação em outros sistemas.

e) Realização de teste de exportação completa, com validação de integridade, como parte das rotinas de disaster recovery.

f) O Backup deve ser incremental.

8. Atualizações tecnológicas tratadas como incidentes

"(Ref.: Apêndice A, item 6.2.19 – "Atualizações tecnológicas registradas como incidentes")

Solicitamos esclarecimento:

O referido item se aplica a atualizações corretivas e evolutivas de software, ou às atualizações da infraestrutura cloud? No modelo SaaS, as atualizações fazem parte do serviço contínuo e não configuram incidentes, mantendo a solução sempre atualizada e em conformidade com os padrões de segurança e desempenho."

Resposta ao fornecedor:

A DGTI/SMPG esclarece que o item 6.2.19 será reformulado conforme segue:

REDAÇÃO ATUAL (a ser substituída):
"As atualizações tecnológicas serão registradas como incidentes, seguindo os prazos definidos no IMR..."

NOVA REDAÇÃO:
"*As atualizações tecnológicas devem ser comunicadas previamente à PMPA com antecedência mínima de 02 (duas) horas, incluindo descrição das mudanças, impactos esperados e janela de manutenção. Atualizações serão realizadas em janelas de manutenção acordadas. Eventuais falhas, indisponibilidades ou degradações de desempenho decorrentes de atualizações serão tratadas como incidentes, seguindo os SLAs de severidade definidos no item 6.2.26, com contagem de prazo iniciada a partir da notificação pela PMPA. Atualizações críticas de segurança podem ser aplicadas com janela de comunicação reduzida, mediante justificativa documentada.*"

9. Teste de plano de recuperação de desastres

"(Ref.: Termo de Referência, item 4.5.1.4 – Plano de Continuidade e Recuperação de Desastres)

Solicitamos confirmar o entendimento de que:

Considerando que a solução será ofertada no modelo SAAS em ambiente cloud, a execução do plano de recuperação de desastres é responsabilidade do provedor de nuvem que deve possuir certificações internacionais (ISO 27001, SOC 2, PCI DSS, etc.), sendo que tais certificações comprovam a conformidade não havendo necessidade de realização de teste operacional, uma vez que, por política dos provedores não, é disponibilizado a terceiros."

Resposta ao fornecedor:

O entendimento está parcialmente correto. As certificações (ISO 27001, SOC 2) do provedor de nuvem atestam a recuperação da infraestrutura. O requisito 4.5.1.4, contudo, refere-se ao Plano de Continuidade da aplicação SaaS (de responsabilidade da Contratada). A Contratada deverá fornecer, mediante solicitação, os relatórios e evidências de seus testes de DRP, demonstrando o cumprimento dos RTO e RPO definidos no item 6.1.18, ou apresentar declaração de que realiza testes de DRP.

10. Documentação da base de dados

"(Ref.: Termo de Referência, item 4.8.2 e 4.8.6 – documentação técnica e registros técnicos de customizações)

Solicitamos confirmar o entendimento de que:

Considerando que a solução será contratada na modalidade SaaS, não será necessária a entrega da documentação detalhada da base de dados (modelagem, dicionário e estrutura interna), considerando que tais informações fazem parte da propriedade intelectual da solução e de sua segurança, podendo ser disponibilizada a documentação dos pontos de integração (APIs, mapeamentos, formatos de exportação e importação de dados), garantindo transparência e interoperabilidade, conforme as exigências de auditoria e LGPD."

Resposta ao fornecedor:

A DGTI/SMPG reconhece que o modelo de dados interno detalhado é propriedade intelectual do fornecedor, protegida pela Lei nº 9.609/1998 (Lei do Software) e pela Lei nº 9.610/1998 (Lei de Direitos Autorais).

Contudo, a Administração Pública necessita de transparência técnica para (i) realizar integrações com sistemas corporativos; (ii) executar auditorias de dados e conformidade LGPD; (iii) diagnosticar problemas operacionais; (iv) garantir continuidade em eventual transição contratual.

A PMPA, portanto, aceita que não seja entregue a documentação completa da estrutura interna da base de

dados proprietária. Entretanto, para viabilizar a gestão adequada do contrato, são requisitos mínimos obrigatórios:

a) Documentação completa de APIs (Application Programming Interfaces), incluindo: endpoints disponíveis, métodos, parâmetros, formatos de requisição/resposta, códigos de erro, limites de taxa, exemplos práticos e versionamento.

b) Dicionário de dados dos campos acessíveis pela PMPA, contendo: nome do campo, tipo de dado, tamanho/formato, obrigatoriedade, valores permitidos, descrição funcional e finalidade do tratamento (essencial para LGPD).

c) Modelo lógico (conceitual) das entidades principais utilizadas pela PMPA, apresentando: entidades, atributos relevantes e relacionamentos, em nível suficiente para compreensão funcional (não exige exposição do modelo físico ou código-fonte).

d) Mapeamento de dados pessoais tratados pelo sistema, identificando: categorias de dados, finalidades, bases legais, prazo de retenção e medidas de segurança aplicadas (obrigatório para compliance LGPD Art. 37).

e) Documentação de integrações com sistemas externos, exclusivamente no escopo do contrato com a PMPA, incluindo fluxo de dados, formatos de importação/exportação e especificações técnicas.

11. Transição de contrato

"(Ref.: Termo de Referência, item 4.8.6 – portabilidade e rastreabilidade das alterações)

Solicitamos confirmar o entendimento de que:

Considerando que a solução será contratada na modalidade SaaS, em eventual transição contratual será considerado suficiente a entrega à Administração todos os dados em formato aberto e legível (CSV, JSON, XLSX), uma vez que a infraestrutura e o código-fonte são partes integrantes da solução SaaS proprietária, não havendo transferência de ambiente ou aplicação, mas garantia de extração completa, íntegra e documentada dos dados da Prefeitura."

Resposta ao fornecedor:

O entendimento está parcialmente correto. A Administração confirma que, em virtude da modalidade SaaS, não é exigida a transferência de código-fonte, infraestrutura ou segredos industriais da solução proprietária, conforme item 7.1 do Termo de Referência. Contudo, o entendimento de que apenas a entrega de dados (CSV, JSON, XLSX) seria suficiente para atender ao item 4.8.6 não é aceito. O referido item trata especificamente de 'customizações ou adaptações'. Para garantir a efetiva portabilidade e rastreabilidade dessas alterações, a Contratada deverá entregar, além da base de dados completa, a documentação técnica e funcional (ex: especificações de regras de negócio, fluxogramas, parametrizações e memória de cálculo) referentes a quaisquer evoluções ou customizações desenvolvidas especificamente para a PMPA durante a vigência contratual. O objetivo é assegurar a retenção do conhecimento das regras de negócio, e não a apropriação do software."

12. OAuth / SSO e autenticação centralizada

"(Ref.: Termo de Referência, item 4.1.7 – autenticação integrada ao SSO da Prefeitura)

Solicitamos seja esclarecido:

Deseja-se integração com o SSO institucional da Prefeitura (SAML, OAuth2, LDAP)?
Em caso afirmativo:
• Os endpoints e diretórios de autenticação serão disponibilizados pela Prefeitura?
• Todos os ambientes (produção e homologação) estarão expostos com IPs válidos e acessíveis para integração?

• *Dada a natureza cloud da solução, seria possível adotar autenticação centrada na aplicação SaaS, com protocolos seguros e auditáveis, em substituição à autenticação local, reduzindo dependência de rede e riscos de indisponibilidade?"*

Resposta ao fornecedor:

A DGTI/SMPG esclarece que a integração com SSO institucional é requisito de governança de TIC, visando gestão centralizada de identidades e rastreabilidade de acessos.

A solução deve suportar como mecanismos de autenticação e autorização o padrão OAuth2 e/ou OpenID. Não serão aceitas soluções que realizem autenticação diretamente no AD. Uma implementação de referência já utilizada no ambiente da CONTRATANTE é o software SSO Keycloak da Redhat (livre de licença).

Especificações técnicas, endpoints, etc. serão fornecidos à contratada após assinatura do contrato, através de solicitação com a PROCEMPA.

Nos casos de quando não houver autenticação via SSO (ex.: contingência ou usuários externos sem vínculo):

X.1.1. A aplicação SaaS deve realizar a autenticação via e-mail (e-mail corporativo do usuário, por exemplo) para o usuário. Quando o público alvo for externo, também deve ser utilizada a autenticação via e-mail.

X.1.2. Não serão aceitos sistemas em nuvem que realizem a autenticação dos usuários exclusivamente através de formulário embutido na própria aplicação, seja através de base local de usuários na aplicação ou integrada à rede do CONTRATANTE através de LDAP.

X.1.3. Todas as operações sobre contas (criação, remoção, login, logout, reset de senha, alteração de permissões, etc.) devem ficar registradas em trilha de auditoria, incluindo, pelo menos, o timestamp (data e horário), o IP origem do acesso, a ação executada e o resultado da operação.

13. Medição para validação / versionamento de documentos

"(Ref.: Apêndice A – requisitos funcionais de controle de documentos)

Solicitamos seja esclarecido:

Poderiam detalhar quais tipos de controle de versão e de validação documental são esperados? E qual o objetivo do versionamento dos documentos?
O requisito visa controle interno de versões ou rastreamento formal com assinaturas eletrônicas e auditoria? A definição impacta o escopo técnico de implementação."

Resposta ao fornecedor:

A DGTI esclarece que o requisito de versionamento e validação fundamenta-se nos itens 3.1.2.11 e 3.3.5.6 do Apêndice do Termo de Referência e tem por objetivo garantir a integridade, a rastreabilidade e a auditabilidade dos documentos técnicos e administrativos geridos pela solução.

Especificamente:

a) Objetivo do Versionamento: Assegurar que nenhuma alteração em documentos relevantes (ex: Projetos Básicos, Termos de Referência, Aditivos Contratuais, Memoriais Descritivos) implique na perda da informação anterior. O sistema deve manter o histórico das versões (quem alterou, quando alterou e o arquivo anterior), permitindo a recuperação de versões passadas para fins de auditoria e comparação.

b) Tipo de Controle: Espera-se um controle formal de rastreabilidade. O sistema deve impedir a sobrescrita silenciosa de documentos. Toda substituição de arquivo deve gerar uma nova versão vinculada ao mesmo registro.

c) Validação e Assinatura: Conforme item 3.3.5.6, mecanismos apropriados devem ser empregados para assegurar a integridade. Para documentos críticos que fundamentam despesas ou obrigações contratuais (como medições e aditivos), a solução deve suportar a validação por meio de trilhas de auditoria robustas (identificação inequívoca do usuário responsável) e, preferencialmente, suporte a assinatura digital/eletrônica, garantindo o não-repúdio das ações realizadas.

14. Exportação de banco a qualquer momento

"(Ref.: Termo de Referência, item 3.3.5 e 4.5.1.2 – tutela e segurança de dados)

Solicitamos seja esclarecido:

A exigência de exportação completa do banco refere-se à totalidade da base ou apenas aos dados da Prefeitura? Em ambiente SaaS multicliente, a exportação integral é inviável por política de segregação de dados. É possível garantir a exportação integral apenas dos dados da Prefeitura, de forma segura e auditável através de documentos de extração de dados e relatórios específicos."

R**esposta ao fornecedor:**

A DGTI/SMPG esclarece que a exigência de exportação refere-se exclusivamente aos dados municipais, não à base multicliente. Especificações técnicas:

a) A exportação deve incluir todos os dados municipais: registros transacionais, cadastros, documentos anexados, logs de auditoria, parametrizações e configurações aplicadas.

b) Formatos de exportação em padrões abertos: CSV, JSON, XML ou equivalentes, acompanhados de dicionário de dados e documentação técnica.

c) A exportação deve preservar integridade referencial entre entidades e permitir reimportação em outro sistema sem perda de informações.

15. Migração de bases de dados legadas

"(Ref.: Termo de Referência, item 4.9.2 – carga inicial e migração de dados existentes)

Solicitamos seja esclarecido:
O edital menciona a necessidade de carga inicial e migração de dados legados, quando aplicável. Poderiam confirmar se essa atividade será executada sob demanda, mediante análise prévia das bases atualmente utilizadas pela Prefeitura?
Como a solução SaaS não requer carga manual contínua, a migração se caracteriza como atividade pontual e de implantação, dependente do formato, volume e disponibilidade das bases existentes (ex.: planilhas, bancos SQL, SIGEF).
Essas informações são essenciais para estimar corretamente o esforço técnico, prazo e custo dessa etapa."

Resposta ao fornecedor:

A migração de dados legados (carga inicial) é parte do objeto e o esforço deve estar contemplado nas 250 UST previstas (Item 2 da tabela). Cabe ressaltar que a Solução será implementada em momento inicial dos Programas de Financiamentos, não havendo execução dos primeiros desembolsos. Confirma-se que a execução se dará mediante análise prévia:

a) A PMPA fornecerá os dados legados em formatos abertos (planilhas, CSV, etc.) e, no caso da integração com o SIGEF, API e manual de API.

b) A Contratada realizará a análise de viabilidade e apresentará um Plano de Migração detalhado.

c) A migração será executada conforme o Plano de Migração aprovado pela PMPA.

16. Documentação técnica do projeto de implantação

"(Ref.: Termo de Referência, item 4.8.2 e 4.12 – plano de trabalho e metodologia)

Solicitamos seja esclarecido: A documentação técnica esperada refere-se à descrição das parametrizações, integrações e cronogramas executados, ou inclui também arquitetura interna da aplicação, que é de propriedade intelectual do fornecedor?
Confirmamos que um plano de trabalho detalhado, com cronograma, ações e resultados entregues, atende plenamente à necessidade de transparência e rastreabilidade previstas no edital."

Resposta ao fornecedor:

A DGTI/SMPG esclarece que a documentação técnica exigida não inclui propriedade intelectual do fornecedor (código-fonte, algoritmos, arquitetura interna do SaaS). A documentação obrigatória refere-se exclusivamente a:

a) Plano de Trabalho executado, incluindo: cronograma real de atividades, marcos atingidos, produtos entregues, equipe alocada e registro de decisões técnicas.

b) Parametrizações realizadas no sistema para a PMPA, documentando: configurações aplicadas, valores de parâmetros, regras de negócio implementadas e justificativas técnicas.

c) Configurações de infraestrutura e ambiente, incluindo: arquitetura de implantação, URLs de acesso, configurações de segurança (firewall, certificados SSL), políticas de backup e retention.

d) Integrações implementadas com sistemas corporativos da PMPA (especialmente SIGEF), detalhando: arquitetura de integração, fluxo de dados, APIs utilizadas, periodicidade, tratamento de erros e procedimentos de monitoramento.

e) Customizações e adaptações realizadas especificamente para a PMPA, com descrição funcional, impactos e dependências.

f) Dados de acesso e credenciais administrativas, usuários de serviço para integrações, tokens de API e certificados digitais (entregues em envelope lacrado à equipe de TI da PMPA).

g) Manuais operacionais para administradores do sistema, incluindo: gestão de usuários e perfis, parametrizações configuráveis, procedimentos de backup/restore, troubleshooting comum e contatos de suporte.

17. Catálogo de dados

"(Ref.: Apêndice A – requisito de catálogo de dados e interoperabilidade)

Solicitamos confirmar o entendimento de que:

O catálogo de dados exigido refere-se apenas ao mapeamento dos campos e integrações relativas à Prefeitura, considerando que por motivos de segurança e sigilo técnico, não é possível expor o modelo integral de dados da aplicação SaaS,
podendo ser fornecido o mapeamento das integrações e exportações de forma integral."

Resposta ao fornecedor:

A DGTI/SMPG confirma que o catálogo de dados exigido refere-se ao mapeamento dos dados municipais tratados no sistema, não à estrutura completa do banco de dados proprietário do SaaS. Especificações técnicas obrigatórias:

a) Inventário de entidades e campos utilizados pela PMPA, incluindo: nome técnico, nome funcional (legível), tipo de dado, tamanho/formato, obrigatoriedade, valores permitidos, descrição e finalidade.

b) Mapeamento de dados pessoais (essencial para LGPD), identificando: categorias de dados pessoais tratados (comum, sensível, criança/adolescente), finalidades específicas de cada tratamento, bases legais (Art. 7º ou 11 da LGPD), compartilhamentos realizados, prazo de retenção, medidas de segurança aplicadas e responsável pelo tratamento.

c) Metadados dos campos: origem do dado, transformações aplicadas, regras de validação, dependências e relacionamentos com outras entidades.

d) Documentação de fluxo de dados: ciclo de vida da informação desde a entrada no sistema até eventual descarte, incluindo processamentos, armazenamentos e transmissões.

e) Catálogo de APIs e integrações, detalhando campos enviados/recebidos em cada integração, formatos e protocolos utilizados.

f) Matriz de privacidade consolidada, relacionando: processos de negócio, dados tratados, finalidades, bases legais, compartilhamentos e riscos.

O catálogo deve ser entregue em formato editável (planilha ou ferramenta de gestão de metadados) e mantido atualizado durante toda a vigência contratual.

18. Documentação técnica do projeto de implantação

"(Ref.: Apêndice A – requisito de API de auditoria e rastreabilidade)

Solicitamos confirmar o entendimento de que:

A API de auditoria deve permitir apenas consulta a logs e registros de ações , mas não de gravação externa por outros sistemas, considerando que em soluções SaaS as operações de gravação externa podem comprometer segurança e rastreabilidade. Desta forma, as consultas autenticadas a logs e relatórios de auditoria atenderiam plenamente ao requisito."

Resposta ao fornecedor:

A DGTI/SMPG confirma o entendimento do fornecedor. A API de auditoria deve ser exclusivamente de CONSULTA (read-only), vedando operações de gravação, alteração ou exclusão de logs por sistemas externos. Especificações técnicas:

a) A API deve permitir consulta programática a logs e eventos de auditoria através de protocolo HTTPS/REST, com autenticação via token ou certificado digital.

b) Dados obrigatórios em cada registro de auditoria: (i) identificação única do evento (ID), (ii) usuário autenticado (login/CPF), (iii) data e hora com timezone (ISO 8601), (iv) endereço IP de origem, (v) tipo de ação/operação, (vi) entidade/objeto afetado, (vii) dados anteriores e posteriores (em caso de alteração), (viii) resultado da operação (sucesso/falha), (ix) sessão/transação.

c) A API deve suportar filtros e pesquisas por: período, usuário, tipo de operação, entidade, resultado e IP de origem.

d) Capacidade de exportação em lote para fins de análise e integração com ferramentas de SIEM/análise de logs corporativas.

e) Retenção de logs pelo prazo mínimo de 5 (cinco) anos ou conforme legislação específica aplicável, o que for maior.

f) Logs de auditoria devem ser imutáveis e protegidos contra alteração, com mecanismos de integridade

(hashing, assinatura digital ou equivalente).

g) Vedação expressa de operações de gravação, alteração ou exclusão de logs através da API ou qualquer outro meio externo.

19. Lista de relatórios e características

(Ref.: Termo de Referência, item 3.3.4 e 3.3.4.1 - relatórios técnicos e financeiros por financiador)

Solicitamos:

Poderia ser disponibilizada lista preliminar dos relatórios obrigatórios por organismo financiador (BID, BIRD, CAF, KfW)? Essa informação é essencial para estimar adequadamente o esforço de desenvolvimento e customização dos relatórios automáticos.

Resposta ao Fornecedor:

Em atendimento à solicitação, foi disponibilizada lista preliminar dos relatórios obrigatórios por organismo financiador, BID, BIRD, CAF e KfW, que constará em arquivo Anexo. Por fim, foi acrescentada a seção 3.3.4.2 ao texto do Termo de Referência para referenciar o Anexo em que constará a lista preliminar.

20. Auditoria com registro de IPs de acesso

"(Ref.: Apêndice A – requisito de segurança e auditoria de acessos)

Solicitamos esclarecer:

O edital prevê que a solução deve realizar auditoria com registro do endereço IP de acesso dos usuários. Poderiam esclarecer qual a finalidade prática esperada para o uso desses registros de IP, considerando que todas as movimentações e operações do sistema já são vinculadas a um usuário autenticado, com registro completo de data, hora, ação executada e demais metadados de auditoria?
No modelo SaaS multicliente, o controle de identidade é realizado por meio de camadas robustas de autenticação e autorização, garantindo total rastreabilidade e responsabilização individual sem dependência do endereço IP.
Dessa forma, gostaríamos de confirmar se o objetivo do requisito é apenas complementar a rastreabilidade já existente (por exemplo, para fins estatísticos), ou se existe alguma obrigação regulatória específica que exija o registro de IP — visto que, em muitos casos, esse dado pode variar conforme o provedor de rede ou o uso de conexões móveis, não representando necessariamente a origem real do usuário."

Resposta ao fornecedor:

A DGTI/SMPG mantém a exigência de registro de endereço IP de origem nos logs de auditoria. Esclarecimentos sobre a finalidade:

a) Finalidade primária: Segurança da informação e detecção de ameaças. O IP permite identificar: acessos de localizações geográficas incomuns, múltiplos logins simultâneos do mesmo usuário de IPs distintos (possível comprometimento de credenciais), tentativas de acesso de IPs bloqueados ou maliciosos conhecidos.

b) Finalidade secundária: Análise forense e investigações. Em caso de incidentes de segurança, fraudes ou irregularidades, o IP é elemento essencial para rastreamento, identificação de origem e produção de evidências para ações disciplinares ou judiciais.

c) Complementaridade com autenticação: O registro de IP não substitui a autenticação de usuário, mas complementa a trilha de auditoria. A identificação do usuário autenticado permanece como elemento principal; o

IP é dado adicional de contexto.

d) Integração com SIEM: O IP permite correlação de eventos entre diferentes sistemas no SIEM corporativo da PMPA, facilitando detecção de campanhas de ataque coordenadas.

e) Conformidade regulatória: Diversas normas de segurança (ISO 27001, controles CIS, frameworks de auditoria do TCU/CGU) recomendam registro de IP como boa prática de auditoria e controle de acesso.

f) Reconhecemos que IPs dinâmicos e uso de VPN limitam a eficácia do controle, mas não eliminam seu valor para análises estatísticas, detecção de anomalias e investigações forenses.

21. Autorização prévia para atualizações de versão e manutenção evolutiva

"(Ref.: Termo de Referência, itens 4.5.1.3 e 4.8.5, e Apêndice A, item 6.2.19

Solicitamos confirmar o entendimento de que:

O edital prevê que atualizações, correções e evoluções da solução devem ser previamente autorizadas pelo contratante.

Considerando que a solução será fornecida na modalidade SaaS multicliente, gostaríamos de confirmar se essa exigência realmente se aplica a esse modelo de fornecimento.

Considerando que em uma solução SaaS as atualizações fazem parte do ciclo natural de manutenção e melhoria contínua da plataforma, garantindo estabilidade, segurança e evolução tecnológica de forma uniforme para todos os clientes.

Diante disso, gostaríamos de confirmar se o objetivo do edital poderia ser plenamente atendido por meio de uma janela padronizada de atualizações, definida em comum acordo com a Administração, com comunicação prévia de cada manutenção, mas sem necessidade de autorização específica para cada liberação de versão.

Esse modelo permitiria conciliar a previsibilidade desejada pela Administração com a continuidade operacional que uma solução SaaS exige.

A necessidade de solicitar autorização individual antes de cada atualização implicaria um forte limitador operacional, reduzindo a velocidade de resposta e a capacidade de entrega contínua que o modelo SaaS exige para atender múltiplos clientes de maneira simultânea e padronizada.

Por essa razão, propomos confirmar que o requisito de autorização prévia não se aplica às atualizações técnicas e corretivas de rotina, permanecendo o dever de comunicação antecipada e documentada ao contratante sempre que houver manutenção programada."

Resposta ao fornecedor:

O requisito de autorização prévia (item 6.2.5) não será mantido, confirmando o entendimento do dever de comunicação antecipada e documentada ao CONTRATANTE quanto houver atualização evolutiva e manutenção programada, não se aplicando às atualizações corretivas técnicas de rotina.

22. Transição contratual e "internalização" da solução SaaS

"(Ref.: Termo de Referência, item 4.15.3 — Plano de Transição Contratual)

4.15. Transição contratual 4.15.3. Até o início do período definido no item anterior, a CONTRATADA deverá apresentar à CONTRATANTE um Plano de Transição Contratual contendo, de forma clara, as atividades, prazos e responsáveis para o repasse de informações, dados e configurações. Caso a Administração opte, ao final do contrato, pela aquisição da solução, o plano deverá ser ajustado para contemplar a internalização do sistema.

Trata-se de contratação de solução tecnológica integrada, na modalidade Software como Serviço (SaaS) - Licença de Uso da Solução Tecnológica. A essência da contratação - Licença de Uso da Solução Tecnológica de forma não exclusiva, intransferível e limitada à vigência do contrato, conflita com qualquer pretensão voltada a aquisição da solução. Faz-se necessário esclarecimento e confirmação de que a transição final contemplará tão somente a entrega das versões finais da documentação, a exportação completa e integral de todos os dados gerados e armazenados durante a vigência contratual, e não a aquisição da solução e internalização do sistema.

Solicitamos esclarecer que a transição contratual não pressupõe cessão, transferência, clonagem, disponibilização ou instalação da solução em si, mas apenas a portabilidade completa dos dados e registros, conforme previsto na LGPD e nas boas práticas de encerramento de contrato em serviços SaaS. Ou seja, não haverá aquisição da solução pelo órgão.

Reiteramos nossa intenção de colaborar para o bom andamento do processo, buscando alinhamento técnico e clareza para formulação de propostas compatíveis com as expectativas da Administração."

Resposta ao fornecedor:

O objeto da contratação é 'Software como Serviço (SaaS) , que consiste em 'Licença de Uso da Solução Tecnológica'. A menção à 'aquisição da solução' e 'internalização do sistema' no item 4.15.3 será desconsiderada, pois é incompatível com a modalidade SaaS. Confirma-se que a transição contratual (item 4.15.1) contemplará a exportação completa e integral dos dados da PMPA em formato aberto e a entrega da documentação, não havendo aquisição de código-fonte ou internalização da aplicação.

Atenciosamente,

Documento assinado eletronicamente por **Eduardo Hack**, **Membro de Comissão**, em 27/11/2025, às 16:10, conforme o art. 1º, III, "b", da Lei 11.419/2006, e o Decreto Municipal 18.916/2015.

Documento assinado eletronicamente por **Lucas Santos de Oliveira**, **Membro de Comissão**, em 27/11/2025, às 16:28, conforme o art. 1º, III, "b", da Lei 11.419/2006, e o Decreto Municipal 18.916/2015.

Documento assinado eletronicamente por **William Quadros Kraemer**, **Membro de Comissão**, em 27/11/2025, às 16:29, conforme o art. 1º, III, "b", da Lei 11.419/2006, e o Decreto Municipal 18.916/2015.

Documento assinado eletronicamente por **Leticia Novello Cezarotto**, **Presidente de Comissão**, em 27/11/2025, às 16:31, conforme o art. 1º, III, "b", da Lei 11.419/2006, e o Decreto Municipal 18.916/2015.

A autenticidade do documento pode ser conferida no site http://sei.procempa.com.br/autenticidade/seipmpa informando o código verificador **36800002** e o código CRC **7B21CDBB**.