

ANEXO XI – DECLARAÇÃO DE REQUISITOS TÉCNICOS OBRIGATÓRIOS

_____, inscrito no CNPJ nº _____, por intermédio de seu representante legal o (a) Sr. (a) _____, portador(a) da Carteira de identidade nº: _____ e do seu CPF nº: _____, DECLARA expressamente sob as penalidades cabíveis, para fins de participação no Pregão Eletrônico Nº _____/_____, que a solução ofertada atende os requisitos técnicos obrigatórios listados abaixo:

1. Considerando a tecnologia desejada pelo MUNICÍPIO, a solução (sistemas) a ser fornecida deve(m):
 - 1.1. Ser implementada para ambiente web, ser multiusuários e multitarefas;
 - 1.2. Permitir acesso às consultas e serviços, em tempo real, em qualquer um dos navegadores atuais, sempre nas suas versões mais recentes;
 - 1.3. Deve suportar os navegadores Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome e outros que venham a ocupar posição relevante nos rankings globais dos navegadores mais utilizados;
 - 1.4. Ser acessível, de modo responsivo, através de navegadores padrão (por exemplo: Google Chrome no Android e Safari no iOS) instalados em dispositivos móveis (smartphones, tablets, etc.);
 - 1.5. Dispensar a instalação de plugins, emuladores ou runtimes para sua utilização;
 - 1.6. Possibilitar serem integrados ao Sistema de Gestão em uso pelo Município sem implicar em qualquer custo adicional para o desenvolvimento destas integrações;
 - 1.7. Disponibilizar todos os serviços internos da aplicação na forma de uma API Rest que possa ser acessada por outras aplicações;
 - 1.8. Ter suporte a serviços Web SOAP, para satisfazer os requisitos técnicos de segurança e robustez necessários à implementação dos serviços acionados e prestados remotamente, incluindo as solicitações de processamento em lote;
 - 1.9. Disponibilizar API homogênea em conformidade com o estilo arquitetural REST (Representational State Transfer) para acesso às rotinas implementadas no sistema, possibilitando a utilização dos serviços por outros aplicativos e sistemas;
 - 1.10. Implementado utilizando a arquitetura de micros serviços, onde cada sistema poderá ser executado de forma separada, inclusive em servidores ou máquinas virtuais diferentes;
 - 1.11. Deverá permitir que várias instâncias do mesmo sistema sejam executadas simultaneamente, a fim de garantir a escalabilidade durante períodos de picos, com muitos acessos, bem como permitir desativar instâncias em períodos com poucos acessos, a fim de

liberar recursos nos servidores.

- 1.12.** Deve ser possível realizar os procedimentos de ativação ou desativação de instâncias sem que seja necessário o shutdown e restart completo de toda a aplicação;
 - 1.13.** A solução deve manter armazenado em banco de dados relacional toda parametrização dos sistemas, dados e fórmulas utilizadas pelas rotinas em sua integralidade; e
 - 1.14.** O modelo de dados deverá seguir as seguintes regras:
 - 1.14.1.** O banco de dados deve possuir padronização quanto à nomenclatura dos objetos (tabelas, colunas, funções, gatilhos, sinônimos, pacotes, domínios, visões, etc.), possuindo nomes claros e de fácil identificação do cadastro, campo ou funcionalidade referenciada;
 - 1.14.2.** Todas as tabelas devem possuir chave primária;
 - 1.14.3.** Em todos os campos que fazem referência a outras tabelas devem existir chaves estrangeiras;
 - 1.14.4.** Nos campos que possuem domínio pré-definido pela aplicação, devem existir restrições (constraints) ou utilizar tipos de dados específicos para gerenciamento do domínio, evitando que sejam inseridos registros com valores que não pertençam ao domínio;
 - 1.14.5.** Todos os objetos do banco de dados devem possuir comentários descrevendo sua utilização e função no sistema;
 - 1.14.6.** O banco de dados deve possuir índices nos objetos relacionados às principais consultas das rotinas da aplicação e nos campos que referenciam outras tabelas, bem como em chaves únicas.
- 2.** Visando garantir o sincronismo de informações entre os sistemas, no processo de integração com o Sistema de Gestão, deverá ser possível implementar as seguintes integrações:
- 2.1.** Importação dos dados dos contribuintes e suas operações a partir do Sistema de Gestão para os sistemas da Solução;
 - 2.2.** Importação do cadastro geral de serviços com as respectivas alíquotas a partir do sistema de Gestão do Município para os sistemas da Solução;
 - 2.3.** Importação do cadastro de feriados do sistema de Gestão do Município para os sistemas da Solução;
 - 2.4.** Importação dos índices de correção monetária e demais parâmetros utilizados no sistema de Gestão do Município para o cálculo de acréscimos de guias de arrecadação, permitindo que os mesmos cálculos de acréscimos utilizados nas guias geradas pelo sistema de Gestão sejam replicados nos sistemas da Solução;
 - 2.5.** Importação, a qualquer momento, a partir da base de dados do Sistema de Gestão, da situação atualizada das guias de pagamento;
 - 2.6.** Exportação, a qualquer momento dos dados relativos às guias de pagamento geradas

pelos

- 2.7. sistemas da Solução, contemplando juros, multa e correção monetária calculados para o Sistema de Gestão;
 - 2.8. Permitir o gerenciamento dos processos de integração a partir de telas do próprio sistema, acessíveis apenas pelo usuário administrador ou suporte técnico; e
 - 2.9. Permitir configurar a periodicidade temporal para importações e exportações de dados.
3. Visando garantir a segurança no acesso e no tráfego de informações, a Solução (sistemas), deverá:
 - 3.1. Permitir autenticação dos usuários em base de dados da própria solução. As senhas devem ser armazenadas utilizando-se de dispersão criptográfica (hash), evitando a leitura, captura via log, interceptação ou exposição da senha original a qualquer momento.
 - 3.2. Utilizar como método de autenticação o padrão OAuth, que implementa a geração de um token de acesso para cada usuário, que precisará ser renovado periodicamente para que usuário continue acessando o sistema sem precisar efetuar novo login;
 - 3.3. Adotar, para o tráfego das informações, método seguro de criptografia e comunicação de dados transmitidos via internet mediante o protocolo Secure Sockets Layer (SSL);
4. Visando garantir um nível adequado para os serviços (Service Level Agreement – SLA) de infraestrutura computacional e segurança dos dados, a infraestrutura disponibilizada deve permitir:
 - 4.1. A hospedagem das aplicações (sistemas) e dados a serem gerados pelo uso dos sistemas da Solução;
 - 4.2. Manter uma disponibilidade de, pelo menos, 99,5%, oferecendo garantia de operação durante vinte e quatro horas por dia, sete dias por semana;
 - 4.3. Manter cópia de segurança da aplicação e dos dados de maneira a garantir a recuperação em quaisquer situações;
 - 4.4. Manter cópias de segurança com periodicidade, no mínimo, de cópias de segurança (backup) diárias incrementais e cópias de segurança semanais completos (full);
 - 4.5. Garantir a segurança dos dados através de equipamentos com recursos de proteção de acesso aos servidores (firewalling) e de detecção de intrusão, garantindo a integridade e confidencialidade dos dados;
 - 4.6. Garantir o acesso remoto (virtual) aos equipamentos a qualquer momento que se fizer necessário. Este acesso deverá ser franqueado aos servidores públicos municipais e aos prestadores de serviços vinculados ou contratados pelo Município;
 - 4.7. O armazenamento dos dados controlados para acesso em tempo real por no mínimo 2 (dois) anos, inclusive os logs de uso, podendo as informações de períodos anteriores serem armazenadas em backups;

_____, _____ de _____ de 2025.

ASSINATURA DO REPRESENTANTE LEGAL

