



ANEXO II – ESPECIFICAÇÕES DA APLICAÇÃO

1. APLICAÇÃO

1.1. Para os fins deste documento, os termos aplicação, software e sistema têm o mesmo significado, referindo-se ao programa de gestão administrativa que será desenvolvido, implantado e mantido pela Contratada.

1.2. Esse sistema deve abranger todos os módulos necessários à administração pública municipal, permitindo que diferentes áreas da Prefeitura e da Câmara possam trabalhar de forma integrada e segura.

2. EXECUÇÃO, SEGURANÇA E COMPATIBILIDADE

2.1. Plataforma e Forma de Funcionamento

2.1.1. O sistema de gestão deverá funcionar inteiramente pela internet (plataforma web), permitindo que os usuários acessem suas funcionalidades diretamente de um navegador, sem necessidade de instalar programas adicionais nos computadores.

2.1.2. O sistema deverá ser compatível com os navegadores mais utilizados, como Mozilla Firefox, Google Chrome, Microsoft Edge, Apple Safari e Opera, sempre em suas versões atualizadas. Caso algum navegador seja descontinuado, a compatibilidade com ele poderá ser dispensada.

2.1.3. Não será permitido o uso de sistemas antigos do tipo cliente-servidor (duas camadas), mesmo que adaptados para rodar no navegador ou por meio de áreas de trabalho remotas (como RDP ou VNC). Essa exigência evita problemas de desempenho e segurança.

2.1.4. O sistema deverá ser desenvolvido com tecnologias modernas e apropriadas para aplicações web, tais como HTML, CSS, JavaScript, PHP, Java, C# ou Python, ou linguagens equivalentes, garantindo desempenho, segurança e escalabilidade.

2.2. Arquitetura e Desempenho

2.2.1. O sistema deverá operar com arquitetura baseada em microsserviços, ou seja, será composto por pequenos módulos independentes que se comunicam entre si. Isso traz maior estabilidade, pois se um módulo falhar, os demais continuam funcionando normalmente.

2.2.2. A aplicação deverá ser multiusuário, permitindo que diversas pessoas acessem e utilizem o sistema simultaneamente, e multitarefa, de forma que várias operações possam ocorrer ao mesmo tempo sem afetar a experiência de outros usuários.

2.2.3. O tráfego de dados entre o computador do usuário e o servidor deverá ser otimizado, transferindo apenas o que for necessário para reduzir o consumo de internet e melhorar o tempo de resposta.

2.2.4. As validações básicas, como verificação de CPF, CNPJ e campos obrigatórios, devem ocorrer diretamente no navegador (lado cliente), tornando a utilização mais ágil.



2.3. Acesso e Segurança na Comunicação

2.3.1. O acesso ao sistema deverá ocorrer por um único endereço na internet (domínio ou subdomínio exclusivo) da Contratada, destinado especificamente à Contratante. Isso garante organização, segurança e facilidade de uso.

2.3.2. Serão permitidos outros endereços apenas para serviços técnicos adicionais — como acesso ao banco de dados, painel de monitoramento (dashboard) ou backup — desde que devidamente protegidos.

2.3.3. Todos os acessos deverão utilizar protocolos de segurança, como HTTPS (em vez de HTTP) e S FTP (em vez de FTP), para criptografar as comunicações e evitar interceptação de dados.

2.4. Interface e Facilidade de Uso

2.4.1. O sistema deverá apresentar-se ao usuário de forma transparente e intuitiva, sem necessidade de alternar entre sistemas ou domínios diferentes para executar tarefas.

2.4.2. O sistema deverá permitir o uso de múltiplas janelas simultâneas, possibilitando que o usuário consulte informações ou trabalhe em mais de um módulo sem precisar sair da aplicação.

2.4.3. A cada ação executada (como salvar, excluir ou alterar informações), o sistema deverá informar imediatamente o resultado, com mensagens visuais claras de sucesso, erro ou alerta.

2.4.4. Nos formulários de preenchimento, o sistema deverá permitir consultar e selecionar dados relacionados diretamente do campo em uso (por exemplo, selecionar um credor ou fornecedor sem sair da tela atual). Se o usuário possuir permissão, deverá também poder cadastrar um novo registro e utilizá-lo imediatamente.

2.4.5. O sistema deverá permitir o envio (upload) de arquivos para seu repositório on-line, aceitando arquivos de pelo menos 2 MB por anexo, ou tamanhos superiores quando necessário;

2.4.6. A aplicação deverá seguir as diretrizes de acessibilidade digital (WCAG 2.1 nível AA).

2.5. Compatibilidade Técnica e Restrições

2.5.1. O sistema deverá funcionar corretamente sem a necessidade de plugins, run-times ou extensões adicionais, exceto nos casos em que houver necessidade de integração com dispositivos externos, como biometria, impressoras ou certificados digitais.

2.5.2. Nesses casos específicos, os recursos utilizados devem ser compatíveis com o sistema operacional Linux, na distribuição Ubuntu 22.04 LTS ou superior, que oferece suporte de longo prazo.

2.5.3. Na camada do navegador, o sistema deve utilizar somente padrões amplamente reconhecidos, como HTML, CSS e JavaScript.



2.6. Integração e Unificação dos Módulos

2.6.1. Todos os módulos do sistema deverão funcionar de forma integrada, compartilhando os mesmos cadastros e dados.

2.6.2. Isso significa que o usuário não precisará exportar ou importar informações entre módulos, nem alternar entre sistemas diferentes para executar tarefas em secretarias, fundos, câmaras ou autarquias.

2.6.3. O sistema deverá possuir um Cadastro Único, que concentre e compartilhe dados básicos com todos os módulos, contendo no mínimo:

- a) Pessoas físicas e jurídicas;
- b) Textos jurídicos (leis, decretos, portarias, etc.);
- c) Centros de custo e organogramas;
- d) Entidades, fundos e órgãos;
- e) Bancos, agências e tributos;
- f) Moedas, cidades, bairros e logradouros;
- g) Produtos e serviços;
- h) Cadastro Brasileiro de Ocupações (CBO);
- i) Assinantes de relatórios.

2.6.4. O sistema deverá impedir a exclusão de informações que estejam ligadas a outros registros ativos, preservando a integridade das bases de dados.

2.7. Consistência e Confiabilidade dos Dados

2.7.1. O sistema deverá possuir ferramentas automáticas de verificação e consistência de dados, capazes de detectar e corrigir inconsistências causadas por falhas ou por importação de dados de sistemas antigos.

2.7.2. Deverá gerar relatórios de inconsistências, indicando o tipo e a gravidade do problema, e registrar logs das execuções para rastreabilidade.

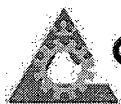
2.7.3. As verificações poderão ser executadas em primeiro plano (visível) ou segundo plano (em background), devendo o usuário ser notificado ao término do processo.

2.8. Cálculos e Parametrizações

2.8.1. O sistema deverá permitir configurar fórmulas de cálculo personalizadas, possibilitando que a Contratante ajuste regras conforme necessidade administrativa.

2.8.2. As fórmulas deverão permitir operações com variáveis, execução de funções pré-definidas (API interna) e exibição do histórico de alterações, com comparação entre valores antigos e novos.

2.9. Segurança de Dados e Transações



2.9.1. O sistema deverá garantir segurança completa em todas as camadas, desde a interface do usuário (front-end) até o armazenamento no servidor, com uso de criptografia, controle de acessos e autenticação segura.

2.9.2. O sistema deverá adotar o conceito de controle de transações, ou seja: ou todas as etapas de uma operação são gravadas corretamente ou nenhuma é, prevenindo erros e corrupção de dados.

2.9.3. O sistema deverá permitir acesso ilimitado de usuários simultâneos, sem necessidade de compra de licenças adicionais para uso dos sistemas básicos (como banco de dados e sistema operacional).

2.9.4. O banco de dados deverá ter restrições de segurança que impeçam acessos indevidos. O sistema não poderá se conectar com o usuário administrador (DBA), devendo haver usuários específicos e controlados para cada função.

2.10. Relatórios e Exportações

2.10.1. O sistema deverá permitir a emissão e visualização de relatórios diretamente na tela, com opção de impressão, assinatura digital e exportação para diversos formatos: PDF, DOCX, XLSX, ODT, ODS, CSV e TXT.

2.11. Controle e Gerenciamento de Usuários

2.11.1. O sistema deverá ter um Gerenciador Central de Usuários, permitindo que todos os acessos — tanto de servidores públicos quanto de cidadãos — sejam controlados em um único painel administrativo.

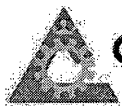
2.11.2. Esse gerenciador deverá permitir:

- a) Criação e atribuição de perfis de acesso (operacional, gerencial, consulta etc.);
- b) Controle de permissões por ação (consultar, incluir, alterar, excluir);
- c) Bloqueio automático após várias tentativas de login malsucedidas;
- d) Armazenamento seguro de senhas criptografadas (por hash, como SHA);
- e) Autenticação via CPF e senha, e-CPF/e-CNPJ, biometria ou Login Único Gov.Br;
- f) Envio automático de mensagens e redefinições de senha por e-mail;
- g) Controle de expiração de senhas e notificações de segurança;
- h) Alertas de tentativas de acesso indevidas com exibição do histórico de logins.

2.11.3. O sistema deverá também permitir o cadastro de usuários externos (como cidadãos e contribuintes), com controle de permissões e integração ao Cadastro Único.

2.11.4. O administrador local poderá atribuir privilégios conforme o organograma, limitando as permissões a subordinados diretos, conforme as regras internas da entidade.

2.12. Conformidade com a Lei Geral de Proteção de Dados (LGPD)



2.12.1. O sistema deverá cumprir integralmente as exigências da Lei nº 13.709/2018 (LGPD), dispondo de mecanismos que assegurem transparência, consentimento e rastreabilidade no tratamento de dados pessoais.

2.12.2. Deverá incluir, no mínimo:

- a) Configuração de termos e condições de uso distintos para usuários internos e externos;
- b) Inventário dos tratamentos de dados pessoais realizados no sistema;
- c) Cadastro de tratamentos realizados em outros meios (digitais ou físicos);
- d) Área pública de transparência ativa, permitindo ao cidadão visualizar como seus dados são utilizados;
- e) Relatórios automáticos de vínculos e interações do cidadão com a entidade;
- f) Registro e verificação de consentimentos dos titulares;
- g) Indicação dos responsáveis locais (Controlador e Encarregado – DPO) com dados de contato;
- h) Solicitação e registro do aceite de políticas de uso e cookies no primeiro acesso;
- i) Web service para que outras aplicações autorizadas consultem o status dos consentimentos registrados;

2.12.3. Conforme definição do art. 5º da Lei 13.709/18, ficam definidos a Contratante como controladora e a Contratada como operadora.

3. CADASTRO DE ENDEREÇOS

3.1. Integração com Base Oficial dos Correios

3.1.1. O sistema deverá possuir integração direta com o Diretório Nacional de Endereços (DNE), mantido pelos Correios.

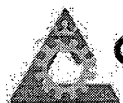
3.1.2. Essa integração garantirá que os endereços informados no sistema estejam em conformidade com o padrão nacional de endereçamento, evitando erros e inconsistências cadastrais.

3.1.3. A base de endereços deverá ser atualizada automaticamente, no mínimo uma vez por mês, para refletir eventuais alterações de logradouros, códigos de CEP e novas localidades criadas.

3.1.4. Sempre que um endereço for informado no sistema, o dado deverá ser validado automaticamente com o DNE.

3.1.5. Se houver divergência (por exemplo, CEP incorreto ou nome de rua inexistente), o sistema deverá alertar o usuário e oferecer a possibilidade de corrigir ou ajustar o endereço antes de concluir o cadastro.

3.2. Atualização Automática e Estrutura de Dados



3.2.1. As tabelas de cidades, estados e países, bem como seus relacionamentos, deverão ser gerenciadas automaticamente pela aplicação, sem necessidade de intervenção manual pelos usuários.

3.2.2. Somente endereços estrangeiros poderão ser cadastrados manualmente, quando não houver correspondência com o DNE.

3.2.3. O sistema deverá permitir a consulta de cidades utilizando, no mínimo, as seguintes chaves de pesquisa:

- a) Nome da cidade;
- b) Nome do estado;
- c) Sigla do estado (UF);
- d) CEP;
- e) Código DNE;
- f) Código da Receita Federal;
- g) Código IBGE.

3.2.4. O uso dessas chaves múltiplas é essencial para cruzar informações com diferentes bases de dados governamentais, que utilizam códigos distintos para identificação de municípios em âmbitos federal, estadual e municipal.

4. CADASTRO DE PESSOAS

4.1. Estrutura Geral

4.1.1. O sistema deverá dispor de um Cadastro de Pessoas completo e flexível, permitindo o registro e gerenciamento de dados de pessoas físicas e jurídicas, utilizados por todos os módulos integrados do sistema.

4.1.2. O cadastro deverá incluir endereços comerciais, residenciais e de correspondência, todos vinculados à base de logradouros para evitar duplicidade ou divergência de informações.

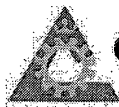
4.1.3. Deverá ser possível definir o tipo da pessoa (física ou jurídica) e registrar múltiplos contatos — telefones residenciais, celulares e e-mails — inclusive mais de um por tipo.

4.2. Funcionalidades Complementares

4.2.1. O sistema deverá permitir o cadastro de dependentes, que também serão tratados como pessoas dentro do sistema, permitindo o uso dessas informações em outros módulos (como benefícios ou relações familiares).

4.2.2. O cadastro deverá incluir os dados de contas bancárias da pessoa, que poderão ser utilizados nas rotinas de pagamento, arrecadação e outras funcionalidades financeiras.

4.2.3. Cada conta bancária deverá ser tipificada conforme sua finalidade (por exemplo, conta-salário, conta de fornecedor, conta de arrecadação).



4.2.4. O sistema deverá permitir o uso de nome social, conforme o Decreto Federal nº 8.727/2016, mantendo registro de log com o motivo e a data da alteração.

4.2.5. Sempre que houver nome social cadastrado, o sistema deverá exibi-lo prioritariamente em todas as telas e relatórios, exibindo o nome civil apenas nas consultas que exijam ambos os registros.

4.3. Registros Profissionais e Rastreabilidade

4.3.1. O sistema deverá permitir vincular a pessoa a órgãos de regulamentação profissional (como OAB, CRC, CRM, CREA, entre outros), armazenando os respectivos números de registro e situação.

4.3.2. Todas as alterações no cadastro deverão ser registradas em histórico próprio (log de auditoria), contendo:

- a) Dados antigos e novos;
- b) Usuário responsável pela alteração;
- c) Data e hora da modificação;
- d) Tipo de operação realizada (inclusão, alteração ou exclusão).

4.3.3. Esse histórico poderá ser visualizado em formato tabular (tabelas com colunas e linhas) ou em formato de linha do tempo, facilitando a auditoria e o acompanhamento.

4.4. Anexos e Documentação Digital

4.4.1. O sistema deverá permitir anexar documentos e arquivos digitais vinculados ao cadastro da pessoa (como RG, comprovantes, certidões, contratos etc.).

4.4.2. Os arquivos deverão ter tamanho mínimo aceito de 2 MB por arquivo, podendo o sistema aceitar tamanhos maiores conforme necessidade.

4.4.3. Não deverá haver limite na quantidade de arquivos que podem ser anexados a uma mesma pessoa.

4.4.4. O envio dos arquivos poderá ser feito por upload direto do computador, ou, quando disponível, por uso de câmera integrada ou seleção de documentos já armazenados no banco de dados.

4.5. Biometria e Segurança de Acesso

4.5.1. O sistema deverá permitir o registro de dados biométricos (digitais) das pessoas, para uso em módulos que exijam autenticação biométrica.

4.5.2. O acesso a essas informações deverá ser restrito aos usuários autorizados, conforme as permissões de cada perfil.

4.6. Autenticidade de Documentos

4.6.1. Todos os documentos eletrônicos emitidos pelo sistema — como alvarás, certidões, certidões negativas, certificados e declarações — deverão possuir mecanismo de verificação de autenticidade online.



4.6.2. Essa verificação deverá ocorrer por meio de link público e código QR Code impresso no próprio documento, permitindo a conferência via smartphone.

4.6.3. Ao acessar o link, o cidadão deverá visualizar uma página de validação contendo os detalhes do documento assinado, inclusive com a opção de baixar o arquivo original para conferência da assinatura digital.

5. ASSINATURA DIGITAL

5.1. Conceito e Finalidade

5.1.1. O sistema deverá permitir o uso de Assinatura Digital Qualificada, conforme definida pela Lei Federal nº 14.063/2020, garantindo validade jurídica aos atos administrativos realizados por meio eletrônico.

5.1.2. A assinatura digital é o mecanismo que comprova a autoria e a integridade de documentos eletrônicos, substituindo a assinatura física em papel.

5.1.3. Essa funcionalidade é essencial para garantir autenticidade, segurança e rastreabilidade nas operações do sistema de gestão pública.

5.2. Situações em que o uso da Assinatura Digital é Obrigatório

5.2.1. O sistema deverá permitir a assinatura digital — na modalidade qualificada — nos seguintes procedimentos e rotinas:

- a) Login ou autenticação no sistema, quando configurado com uso de certificado digital;
- b) Envio de petições eletrônicas e documentos no Processo Administrativo Digital;
- c) Escrituração fiscal e declarações de serviços prestados e tomados;
- d) Assinatura de relatórios, pareceres e documentos administrativos em geral;
- e) Recebimento e envio de processos em meio digital entre setores, órgãos ou entidades;
- f) Assinatura de documentos gerados pelo sistema, inclusive após a emissão de relatórios, possibilitando a assinatura direta no arquivo final.

5.2.2. Essas operações deverão poder ser executadas dentro do próprio sistema, sem necessidade de programas externos, exceto quando for preciso acessar o dispositivo físico do certificado digital (token ou cartão) instalado na máquina do usuário.

5.3. Solicitação e Fluxo de Assinaturas

5.3.1. O sistema deverá permitir a criação de fluxos de assinatura digital, em que um usuário possa:

5.3.2. Solicitar a assinatura de um ou mais documentos a outro usuário;

5.3.3. Acompanhar o andamento da solicitação (pendente, assinada ou rejeitada);

5.3.4. Rejeitar uma solicitação de assinatura, caso discorde do conteúdo do documento.

5.3.5. Dessa forma, é possível organizar o processo de validação de documentos de forma hierárquica, transparente e rastreável, com controle de prazos e responsáveis.

5.4. Carimbos de Assinatura (Estampas Digitais)



5.4.1. O sistema deverá permitir a configuração de carimbos de assinatura digitais personalizadas, utilizados para “estampar” no documento PDF a confirmação de que foi assinado digitalmente.

5.4.2. O carimbo poderá conter:

- a) Texto, como nome do signatário, cargo, data e hora da assinatura;
- b) Imagem, como brasão, logotipo ou selo institucional;
- c) Texto e imagem combinados.

5.4.3. Esses carimbos poderão ser definidos de forma:

- a) Individual, para cada usuário; ou
- b) Institucional, aplicável a toda a entidade.

5.4.4. Deverá ser possível posicionar automaticamente o carimbo nos documentos, ou permitir que o usuário escolha manualmente o local da estampa, em qualquer página do arquivo PDF.

5.4.5. O sistema também deverá permitir que a Contratante personalize completamente o modelo de carimbo, adequando-o ao padrão visual e às normas internas do órgão público.

5.5. Certificados Digitais e Controle de Validade

5.5.1. O sistema deverá ser compatível com certificados digitais A1 (arquivo eletrônico) e A3 (token ou cartão físico), podendo utilizar:

- a) Certificados armazenados localmente na máquina do usuário; e/ou
- b) Certificados armazenados em repositório seguro do próprio sistema.

5.5.2. Antes de realizar a assinatura, o sistema deverá:

- a) Exibir ao usuário a lista de certificados disponíveis (mostrando apenas os pertencentes ao próprio usuário);
- b) Indicar se o certificado está vencido ou inválido;
- c) Emitir alerta caso o usuário tente assinar novamente um documento que já foi assinado, oferecendo a opção de cancelar a nova assinatura.

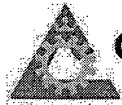
5.5.3. O objetivo é garantir que todas as assinaturas sejam feitas de forma consciente e segura, evitando duplicidade ou erro de autenticação.

5.6. Visualização e Confirmação da Assinatura

5.6.1. Durante o processo de assinatura, o sistema deverá exibir ao signatário o conteúdo completo do documento antes da confirmação, para que ele saiba exatamente o que está assinando.

5.6.2. Em caso de assinatura individual, o documento deverá ser mostrado integralmente na tela.

5.6.3. Em caso de assinatura em lote, o sistema deverá permitir visualizar a lista completa dos documentos relacionados.



5.6.4. Assim, o servidor ou autoridade garante que o ato de assinatura é consciente e auditável.

5.7. Verificação Pública de Autenticidade

5.7.1. Todo documento assinado digitalmente deverá conter, de forma automática, uma estampa de verificação de autenticidade, com:

- a) Um link público (URL) para consulta do documento no portal do sistema; e
- b) Um QR Code legível impresso no arquivo PDF, permitindo a conferência via smartphone.

5.7.2. Ao acessar o link ou o QR Code, o cidadão ou o auditor deverá visualizar uma página de verificação contendo:

- a) Os dados do documento assinado (título, número, tipo, data, signatários);
- b) O status da assinatura digital (válida, expirada ou revogada);
- c) A possibilidade de baixar o arquivo original assinado para conferência da integridade digital.

5.7.3. Esse mecanismo garante transparência, segurança e autenticidade pública, atendendo às exigências da Lei 14.063/2020, da Lei 14.129/2021 (Governo Digital) e da Lei 14.133/2021 (Nova Lei de Licitações e Contratos).

6. ADMINISTRAÇÃO E AUDITORIA

6.1. Finalidade

6.1.1. O sistema deverá oferecer um conjunto completo de ferramentas de administração, auditoria e rastreabilidade de ações, assegurando o controle sobre todas as operações realizadas, desde acessos e modificações de dados até a emissão de relatórios e o envio de comunicações.

6.1.2. Esses recursos são essenciais para garantir segurança, integridade, transparência e responsabilização dos usuários, conforme os princípios da administração pública e da Lei nº 14.133/2021.

6.2. Registro de Auditoria (Logs do Sistema)

6.2.1. O sistema deverá manter múltiplos tipos de registros de auditoria (logs), permitindo rastrear todas as ações realizadas pelos usuários, inclusive as automáticas do próprio sistema.

6.2.2. Os logs deverão registrar, no mínimo:

- a) Ações de consulta, inclusão, alteração e exclusão de dados;
- b) Ações que afetem diretamente o banco de dados;
- c) Eventos de login, logout, falhas de autenticação e bloqueio de acesso;
- d) Operações administrativas do sistema, como configurações ou geração de relatórios.

6.2.3. Cada registro de auditoria deverá conter obrigatoriamente:

- a) Tipo da operação realizada (consulta, inclusão, alteração, exclusão etc.);



- b) Módulo e rotina do sistema em que ocorreu a ação;
- c) Endereço IP da estação de trabalho;
- d) Usuário responsável pela operação;
- e) Data e hora exatas da execução;
- f) Dados novos e antigos (para alterações) e dados excluídos (para exclusões).

6.2.4. Os logs devem ser armazenados de forma segura, protegidos contra exclusão ou modificação, e devem permitir consulta histórica com filtros por usuário, data, tipo de operação e módulo do sistema.

6.2.5. Na visualização:

- a) Inclusões deverão exibir os novos dados inseridos;
- b) Alterações deverão mostrar valores antigos e novos;
- c) Exclusões deverão indicar os dados excluídos e o responsável pela ação.

6.2.6. O administrador local deverá ter acesso a uma interface de gerenciamento de auditoria, com controle de permissões e possibilidade de restringir o acesso a esses registros.

6.3. Gerenciamento de Sessões e Usuários Ativos

6.3.1. O sistema deverá permitir ao administrador local monitorar, em tempo real, as sessões ativas no servidor de aplicação, exibindo:

- a) Data e hora de início da sessão;
- b) Data da última requisição;
- c) Nome e identificação do usuário;
- d) Endereço IP da estação de trabalho;
- e) Tempo total da sessão ativa.

6.3.2. O administrador deverá poder:

- a) Encerrar sessões remotamente, caso necessário;
- b) Enviar mensagens internas para um ou mais usuários conectados, diretamente pelo sistema (por exemplo, avisos de manutenção, prazos ou alertas de segurança).

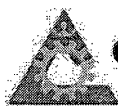
6.3.3. Além disso, o sistema deverá manter um histórico de acessos de todos os usuários, registrando: data, hora, IP, rotina acessada e ação executada.

6.4. Controle e Rastreabilidade de e-mails

6.4.1. O sistema deverá possuir um módulo completo para envio e recebimento de e-mails institucionais, integrado aos demais módulos do sistema.

6.4.2. Deverá permitir:

- a) Configuração de múltiplas contas de e-mail (setores, secretarias, departamentos etc.) em um único local, acessíveis a todos os módulos;



- b) Definição de qual conta será usada por tipo de comunicação (ex: notificações fiscais, ordens de pagamento, comunicações administrativas);
- c) Criação de modelos de mensagens padrão, com textos e assinaturas pré-definidas;
- d) Opção para que o usuário selecione, no momento do envio, a conta desejada, conforme as permissões configuradas;
- e) Acompanhamento do status de cada mensagem enviada (enviada, entregue, falha etc.), em uma espécie de caixa de saída global;
- f) Monitoramento das caixas de entrada para identificar mensagens retornadas com erro ou respostas automáticas;
- g) Notificação automática ao remetente em caso de falha no envio.

6.4.3. Esse controle garante que todas as comunicações enviadas pelo sistema sejam auditáveis, seguras e rastreáveis.

6.5. Controle de Emissão de Relatórios

6.5.1. O sistema deverá garantir total rastreabilidade e controle sobre a emissão de relatórios administrativos e operacionais, com as seguintes funcionalidades mínimas:

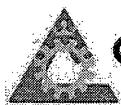
- a) Permitir a emissão simultânea de vários relatórios por um mesmo usuário;
- b) Manter relatórios em execução mesmo que o usuário feche o sistema, enviando uma notificação automática ao término;
- c) Evitar duplicidade de execução quando o mesmo relatório, com os mesmos parâmetros, já estiver em processamento;
- d) Notificar o usuário assim que a emissão for concluída;
- e) Enviar relatórios automaticamente por e-mail, permitindo definir data e hora do envio;
- f) Permitir assinatura digital dos relatórios diretamente pelo sistema;
- g) Armazenar cópia de cada relatório emitido no banco de dados, com código único e informações completas sobre filtros, usuário, data/hora e ID da emissão;
- h) Permitir consulta pública desses relatórios via portal, garantindo a verificação de autenticidade e integridade;
- i) Permitir impressão a partir de dispositivos móveis (Android), especialmente em impressoras térmicas Bluetooth homologadas.

6.5.2. Esses relatórios deverão sempre conter identificação única, marca d'água, brasão institucional, nome da entidade e número de páginas.

6.6. Gerador de Relatórios e Consultas

6.6.1. O sistema deverá dispor de um gerador de relatórios e consultas avançado, com as seguintes capacidades:

- a) Criação, edição e reutilização de formatos de relatórios personalizáveis, incluindo margens, cabeçalhos, rodapés e marca d'água;



- b) Inserção de imagens, códigos de barras e QR Codes;
- c) Criação de novos layouts com base em modelos existentes, inclusive versões temporárias (em homologação);
- d) Controle de versões de relatórios, permitindo restaurar versões anteriores;
- e) Definição de permissões de acesso a relatórios e consultas;
- f) Geração de consultas baseadas em metadados ou instruções SQL;
- g) Opção de definir filtros padrão (default), com parâmetros fixos ou variáveis;
- h) Visualização dos resultados utilizando os mesmos recursos das consultas nativas (filtros, ordenações, impressão etc.);
- i) Possibilidade de marcar consultas como "favoritas", para acesso rápido pelo menu do usuário.

6.7. Agendamento e Automação de Tarefas

6.7.1. O sistema deverá permitir o agendamento de tarefas automáticas, com interface visual e intuitiva, apresentando fluxos no formato de fluxogramas, para:

- a) Emitir relatórios automaticamente;
- b) Verificar registros e condições específicas no banco de dados;
- c) Enviar notificações ou e-mails automáticos;
- d) Executar rotinas periódicas (diárias, semanais, mensais, anuais).

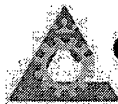
6.7.2. Essas tarefas poderão ser programadas por horário, frequência ou evento e deverão manter um histórico detalhado de execuções, incluindo status e logs de cada atividade.

6.8. Workflow (Fluxo de Processos)

6.8.1. O sistema deverá incluir um módulo de Workflow nativo, sem depender de sistemas externos, desenvolvido no mesmo ambiente e banco de dados da aplicação.

6.8.2. Deverá permitir:

- a) Desenho e execução de processos administrativos conforme a metodologia BPMN (Business Process Model and Notation), incluindo raias horizontais e verticais, eventos e atividades;
- b) Relacionar documentos digitais, textos jurídicos e cadastros do sistema;
- c) Execução automática de tarefas, carregamento de telas e formulários da própria solução;
- d) Controle de ativação, homologação e versionamento dos fluxos, permitindo evolução sem impacto em processos em andamento;
- e) Registro histórico das alterações realizadas nos processos e possibilidade de comparar e restaurar versões anteriores;
- f) Impressão de documentos a partir de dispositivos móveis (Android) via impressoras térmicas Bluetooth, com requisitos técnicos e equipamentos homologados informados pela contratada.



CATAGUASES
PREFEITURA

SECRETARIA DE
FAZENDA

gov.br

Documento assinado digitalmente

FABRICIO ANDRADE CRUZ

Data: 17/10/2025 10:51:12-0300

verifique em <https://validar.it.gov.br>

Fabício Andrade Cruz
Elaboração do Anexo II

