ANEXO II DO TERMO DE REFERÊNCIA – ESPECIFICAÇÕES DA APLICAÇÃO

APLICAÇÃO

Neste instrumento, os termos "aplicação", "software" e "sistema" são tratados como sinônimos, fazendo referência ao arranjo de programas de gestão administrativa projetados pela CONTRATADA, englobando a totalidade de seus módulos operacionais sendo estes do ANEXO B itens OBRIGATORIOS ELIMINATORIOS.

EXECUÇÃO, SEGURANÇA E COMPATIBILIDADE

A ferramenta de gestão precisará operar de forma nativa em ambiente web. O acesso deve ser garantido e integralmente compatível com os navegadores de mercado, tais como Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge e Opera, sempre em suas atualizações mais recentes (excetuando-se hipóteses de descontinuidade de algum navegador). Fica terminantemente proibido o emprego de softwares de arquitetura tradicional (desktop cliente-servidor) que utilizem artifícios de emulação para rodar no navegador, bem como acessos por espelhamento de área de trabalho via protocolos VNC ou RDP. Sendo assim, o desenvolvimento deve repousar sobre linguagens web legítimas (a exemplo de Python, C#, Java, PHP, JavaScript, CSS e HTML).

A interface entregue ao operador precisa ser "transparente", o que significa garantir uma navegação fluida, dispensando a exigência de transitar por múltiplos domínios. Toda a operação fluirá por um único endereço (ou subdomínio) providenciado pela fornecedora e reservado exclusivamente à CONTRATANTE, com a única ressalva para acessos voltados à administração da infraestrutura (como painéis do data center, resgate de backups e gerência do banco de dados). Os canais de conexão devem ostentar protocolos de criptografia e segurança (como SFTP no lugar do FTP e HTTPS em detrimento do HTTP), além de outras certificações vitais de tráfego.

A plataforma deverá conceder o recurso de carregar arquivos (upload) para o armazenamento em nuvem sempre que a rotina cobrar, exigindo-se suporte mínimo e inegociável para anexos de 2 MB (dois megabytes) ou mais por cada arquivo individual. Não se admitirá restrição que imponha limites inferiores a esta margem.

O consumo de dados na comunicação entre o servidor e as máquinas clientes precisará ser otimizado ao extremo para economizar a banda de internet do município. Dentro da premissa cliente-servidor, a maior parcela das validações processuais deve ser transferida para o equipamento do usuário final.

As validações primárias de dados (como o preenchimento de campos obrigatórios, checagem matemática de CNPJ e CPF, dentre outras) ocorrerão obrigatoriamente do lado do cliente (front-end).

Exige-se que o software seja alicerçado em arquitetura de microsserviços, operando de forma multitarefa e multiusuário. O viés multiusuário garante que a ferramenta comporte um vasto número de acessos simultâneos, inclusive permitindo múltiplas sessões abertas pelo mesmo servidor ou por setores distintos. A faceta multitarefa assegura que diversas rotinas rodem em paralelo sem que o acionamento de uma delas paralise o uso de outro módulo ou trave a navegação de terceiros (exceto quando a interrupção for mandatória para preservar a integridade das tabelas do banco). Descolando-se da antiga arquitetura monolítica, o formato em microsserviços assegura que a pane isolada de uma engrenagem não derrube a estabilidade do restante do ecossistema.

É impreterível que todos os módulos convivam numa integração fluida e nativa. O operador inserirá os registros em repositórios unificados, anulando qualquer necessidade de importar ou exportar tabelas e arquivos entre as secretarias, fundos, autarquias e Câmara Municipal. O cruzamento de dados transitará de forma livre entre os compartimentos da solução, sem cobrar do usuário o fechamento de um programa para o ingresso em outro.

Em respeito à inviolabilidade, agilidade e usabilidade, veta-se a imposição de instalação de plugins ou extensões (runtimes) nos computadores locais para fazer o sistema rodar. A exceção aplica-se estritamente àqueles aplicativos pontuais e intermediários, vitais para fazer a ponte com periféricos físicos da prefeitura (como coletores biométricos, leitoras de certificados digitais e impressoras), ou para o diálogo com programas nativos da estação (como editores do pacote Microsoft Office ou visualizadores de arquivos PDF).

Mesmo nestas ressalvas, tais complementos obrigam-se a funcionar perfeitamente no ambiente Linux, especificamente na distribuição Ubuntu em sua versão 22.04 ou superior, desde que enquadrada como LTS (Long Term Support).

Na vitrine do usuário (camada cliente), somente recursos de navegação universais e amplamente difundidos (JavaScript, CSS, HTML) serão empregados, banindo-se exigências de módulos adicionais para o trabalho comum, exceto nas famosas barreiras impostas pelas tecnologias web quanto à restrição de acesso direto aos discos e pastas locais do computador.

O arranjo tecnológico deve portar mecanismos para o trabalho em múltiplas abas e janelas, permitindo que o servidor deixe diversas telas de rotinas abertas simultaneamente para apoiar seu raciocínio de trabalho. Esse recurso facilitará a transição dinâmica entre diferentes entidades da administração ou exercícios financeiros, rechaçando a obrigação de derrubar a sessão ativa para buscar dados em outro segmento.

A plataforma comunicará respostas rápidas (feedback visual imediato) sempre que o servidor realizar uma ação, valendo-se de janelas de aviso, caixas de diálogo ou outras manifestações em tela. Em procedimentos de impacto transacional (inserções, exclusões ou edições no banco de dados), essa confirmação só deve surgir após a finalização da varredura final, atestando de forma clara se a gravação ocorreu com sucesso integral ou se sofreu interrupções.

Durante a digitação em formulários (telas de pesquisa, cadastros ou filtros de relatórios), o sistema oferecerá o preenchimento automático (auto completar) e um atalho direto para a aba de pesquisa do dado conexo. Isso impede que o funcionário abandone seu trabalho em andamento para consultar uma numeração em outro menu do sistema. Caso o usuário, a partir desse atalho de busca da informação cruzada, perceba que ela ainda não existe (ex: a falta de uma ocupação sindical nova no cadastro de pessoa, ou um credor não localizado no momento do empenho), e contanto que possua a devida permissão, a tela concederá a facilidade de realizar a inclusão imediata desse novo registro, selecionando-o em seguida para fechar o formulário original.

O sistema integrará uma inteligência de consistência de dados abrangendo múltiplas áreas. O alvo dessa ferramenta é varrer as matrizes para coibir e acusar falhas estruturais plantadas ao longo do uso diário ou resquícios corrompidos de migrações anteriores, permitindo ao gestor:

Armazenar o rastreio (logs) a cada rodada de limpeza, para atestar se a inconsistência persistiu em face de uma execução anterior;

Gerar listagens impressas com os apontamentos irregulares achados nas averiguações, classificando-os por graus de gravidade;

Viabilizar que essa varredura densa rode nos bastidores (background, em segundo plano no servidor) sem congelar o painel do servidor. Assim que o crivo for encerrado, um aviso pipocará na tela do requisitante.

Haverá a possibilidade de parametrizar as engrenagens de fórmulas e cálculos da aplicação, chancelando os seguintes controles:

A montagem e a execução de variadas operações matemáticas, além da atribuição de pesos e valores a diferentes variáveis;

A utilização de laços lógicos (API) disponíveis para o operador explorar e modelar consoante a urgência do setor;

O acesso livre ao histórico cronológico das modificações, permitindo o confronto visual imediato entre as configurações pretéritas e as vigentes.

A blindagem contra invasões ou acessos indiscriminados aos repositórios será imperativa. Este escudo de segurança manifestar-se-á em sucessivas camadas de defesa: partindo de travas na interação do cliente (front-end), trafegando num duto de comunicação blindado por chaves (HTTPS) e culminando no estreitamento severo dos endereços e portas no núcleo do serviço.

A quantidade de credenciais e usuários em trânsito simultâneo não sofrerá gargalos ou tetos limitadores. A administração pública não será compelida a custear aquisições adicionais de qualquer licenciamento subjacente que suporte o arranjo tecnológico (incluindo gerenciadores de dados e o motor do sistema operacional). A conformidade a esta exigência poderá ser ratificada mediante emissão de Declaração Formal durante a cerimônia de prova de conceito (amostra).

CADASTRO ÚNICO INTEGRADOR

A ferramenta abraçará o conceito matricial do Cadastro Único. Isso consagra o compartilhamento orgânico de tabelas e inibe integrações improvisadas por artifícios frágeis, os quais corriqueiramente danificam a coesão histórica dos registros. A base unificada irradiará as suas referências para toda a totalidade de módulos adquiridos.

A título de especificação basilar, este coração de dados aglomerará e ordenará: matrizes de pessoas físicas e CNPJs; arcabouço normativo (leis, portarias, textos legais); arranjo de organogramas e polos de custo; entes governamentais e dependências; bancos e carteiras de agências; malha tributária; padronização de moedas correntes; árvores de CEP (bairros, cidades e logradouros); dicionário de produtos; o CBO (Cadastro Brasileiro de Ocupações); além da galeria de assinantes qualificados em documentos.

Tencionando munir outras aplicações adjacentes, a tecnologia abrirá conexões (WebServices), calcadas nos protocolos de ponta (SOAP ou REST), entregando os seguintes fluxos de informação (no mínimo):

Malha de Pessoas: Acesso liberado para pesquisar (de forma detalhada ou condensada), editar e injetar informações no agrupamento de Pessoas Físicas e Jurídicas, espraiando os dados imobiliários, propriedades e inscrições econômicas;

Arquitetura Governamental: Canal livre para explorar os braços do organograma, as repartições e o esquema numérico dos centros de custos;

Certificação de Identidade: Prestação do serviço de autenticação logada que permitirá às plataformas satélites da prefeitura (ou parcerias com terceiros autorizados) se utilizarem da exata mesma credencial e senha balizadas no sistema mestre.

A modelagem interna das tabelas chancelará a rigidez de integridade referencial, bloqueando em nível sistêmico e de banco de dados qualquer tentativa de exclusão de cadastros que sustentem vínculos primários com outras rotinas ou atos em operação.

O motor do sistema respeitará o preceito de "transações englobadas" (o processamento só se consagra se alcançar a completude da cadeia; havendo interrupção na rota, tudo volta ao marco zero, eliminando dados mutilados). Essa engrenagem é o pilar que impedirá que curtos elétricos, falhas ríspidas de hardware ou solavancos de sistema comprometam a pureza do repasse de informações.

O operador precisará receber mensagens taxativas informando se a cadeia de eventos processados (edições, deleções ou novos apontamentos) encerrou-se com total êxito ou detectou problemas, restando essa informação clara antes de a plataforma lhe devolver a autonomia para iniciar novos despachos.

As trancas de segurança do SGBD vedarão de forma implacável que agentes sem patente vasculhem os repositórios vitais. O ingresso das requisições geradas pelo sistema jamais será orquestrado utilizando o selo de acesso irrestrito do banco (Superusuário/DBA). A plataforma terá para si um "usuário específico de aplicação" para as conexões padrões, ao passo que outros operadores de níveis secundários disporão de perfis isolados voltados puramente à averiguação e consulta.

Ao longo de todas as frentes modulares da tecnologia, o poder de extrair e exibir informações ofertará ferramentas nativas de visualização primária e, paralelamente, trará opções de impressão física, transferência digital, firmação por meio de assinatura eletrônica iminente e gravação exportada em uma gama de extensões (minimamente: TXT, CSV, ODS, ODT, XLS ou XLSX, DOC ou DOCX e arquivos PDF).

GESTÃO CENTRALIZADA DE USUÁRIOS E SEGURANÇA

O software hospedará um Gerenciador de Usuários central e de ampla autonomia, englobando no mesmo teto a governança das chaves de acesso dos operadores de balcão (funcionários), prestadores terceirizados e contribuintes da rede externa.
Esta central operará as delimitações de perfil e as métricas de segurança mediante as seguintes ferramentas de retaguarda:

- Amarração Funcional: Plugar o indivíduo a ramificações de perfis definidos (tais como Nível Gerencial, Base Operacional, Gestão de Processos ou Crivo de Consultas), admitindo também o desenho de modelos de acesso puramente customizados pela administração;
- Permissões Ramificadas: Explorar os filtros dos perfis para chancelar ou aniquilar o poder de alcance do usuário dentro das rotinas modulares (limitando os graus de visão, inclusão, modificação e eliminação das abas do painel);

- Embargos de Senha: Intervir de forma automatizada e preventiva diante de violações sistêmicas. O mecanismo travará a conta que transpor uma sequência não exitosa de tentativas erradas de inserção da senha (o limite de tentativas será cravado à critério do responsável da Ti);
- Barreira Criptográfica: As credenciais de verificação (senhas) flutuarão na teia da internet e repousarão nos discos munidas de cifras de embaralhamento robustas (hashes padrão SHA ou algoritmos análogos), escondendo a composição das letras de quaisquer olhos curiosos — mesmo em telas de pesquisa do suporte tecnológico interno;
- Segregação de Setores: Vincular as permissões analíticas do usuário estritamente aos recintos competentes, travando ou alargando suas interações baseando-se em sua fixação a determinados Órgãos, Departamentos, Centros de Custos isolados ou visão integral do paço;
- Multipossibilidade de Login: O gestor-mor elegerá os ritos cabíveis para a tela inicial de autenticação, abraçando os moldes de e-CNPJ/e-CPF, cruzamento de Senha e CPF, verificação Biométrica ou ingresso simplificado através do portal oficial Login Único Gov.Br;
- Comunicações Ativas: O motor disporá de gatilhos automáticos para remeter e-mails de recepção no instante exato da filiação de um novo perfil. A grafia, o recado institucional e o visual destas mensagens inaugurais serão integralmente editáveis pelo Município;
- Mensageria Customizada: Prover caixas de aviso para enviar memorandos eletrônicos pontuais (ou via e-mail ou janela intra-sistema) segmentando os envios por usuário exclusivo ou lotes de servidores;
- Reset de Credenciais sem Contato Humano: O titular administrador intervirá na reposição das chaves de segurança da força de trabalho, porém, sem que tenha acesso visual à combinação de caracteres. A recomposição enviará o elo de definição sigilosa direto à caixa de correio do beneficiário da chave, minando interceptações e o acesso indevido aos conteúdos da prefeitura;
- Expiração Estratégica: O núcleo de gestão tecnológica terá o condão de estipular que determinada senha perdeu sua validade. O dono da conta será instado imediatamente a formalizar uma combinação nova já em seu encontro seguinte com a tela de login.

A matriz de coordenação destes apontamentos transcorrerá numa plataforma homogênea, abrangendo na mesma tela os internos das secretarias e os externos dos portais fiscais, resguardando apenas os ditames das escalas hierárquicas necessárias para promover intervenções nestes registros.

Fica assegurada ao cidadão a capacidade de se habilitar nos balcões eletrônicos (Portal/Autoatendimento) abrindo por si mesmo uma credencial originada na estrutura do cadastro único municipal, caso seu CPF/CNPJ ainda não seja reconhecido como usuário válido de portal.

Focado em bloquear vulnerabilidades no que tange ao quadro laboral, a interface fará varreduras iminentes contra a base do setor de RH durante o processo de efetivação do login, abraçando obrigatoriamente as seções abaixo:

- Cancelar de imediato as entradas no banco logístico das chaves cujos contratos não operem como "ativos" nas pastas do Recursos Humanos (repelindo os passos de servidores apartados em gozo de férias prolongadas, demitidos ou de licença em casa);
- Viabilizar que a prefeitura limite a autorização do sistema de modo a emoldurá-la nos trilhos horários do ponto funcional repassado pelo RH, rechaçando expedições em horários descabidos;
- Assumir exigências imutáveis para a arquitetura de senhas do paço (estipulando níveis de complexidades de letras/números e o traçado de caracteres aceitos);
- Atribuir vida útil fixa aos logins, provocando prazos limites de expiração para as senhas de forma generalizada;
- Individualizar, se for o pleito da chefia, o comportamento de vida destas chaves, decidindo se as credenciais de usuários em posições estratégicas jamais perdem a vigência, enquanto dita que outros recadastrem em x dias corridos ou numa data pontual traçada;
- Promover delegação fracionada de privilégios, onde os Secretários ou Diretores receberão aval para distribuir parcelas de seus poderes unicamente aos elos de subordinação inferior na árvore do organograma.

Para garantir transparência profilática, toda a vez que o indivíduo acessar as dependências do software em que a sua retaguarda tiver verificado senhas estouradas ou furos no reconhecimento do CPF, uma caixa de avisos ressaltará de forma ostensiva o rol temporal constando os horários daquelas interceptações falhas na catraca de login.

ASSINATURA DIGITAL

Permitir a utilização de Assinatura Digital na modalidade Qualificada, em conformidade com a Lei nº 14.063/2020, nos seguintes procedimentos e funcionalidades do sistema: autenticação de usuários (login); peticionamento eletrônico; escrituração fiscal; declarações de serviços prestados e tomados; assinatura de documentos digitais em geral; assinatura de documentos gerados após a emissão de relatórios; emissão de pareceres em processos digitais; bem como no recebimento e envio de processos por meio eletrônico.

O sistema deverá possibilitar a assinatura digital de documentos diretamente na própria aplicação, sem a necessidade de utilização de sistemas externos ou ferramentas adicionais, excetuando-se apenas os componentes indispensáveis ao acesso ao dispositivo de leitura do certificado digital instalado na máquina local do usuário.

Deverá permitir a funcionalidade de solicitação de assinatura, por meio da qual um usuário possa encaminhar um ou mais documentos para assinatura de outros usuários do sistema, possibilitando que o destinatário aceite ou rejeite o documento submetido para assinatura.

O sistema deverá permitir a configuração de carimbos de assinatura digital, para uso da Assinatura Digital Qualificada conforme a Lei nº 14.063/2020, podendo ser definidos por usuário ou de forma institucional (para toda a entidade). Deverá ser possível configurar o conteúdo a ser aplicado como “estampa” sobre o documento PDF assinado. O carimbo deverá suportar inserção de textos e imagens, de forma conjunta ou independente, contemplando as seguintes opções:
somente texto;
somente imagem;
texto e imagem combinados.

A personalização do carimbo deverá ser integralmente configurável pela CONTRATANTE, permitindo sua aplicação automática no documento ou posicionamento manual pelo usuário durante o processo de assinatura, diretamente na visualização do documento. O posicionamento deverá ser permitido em qualquer página do documento PDF.

O sistema deverá possibilitar a realização de assinatura digital utilizando certificados armazenados em repositório próprio da aplicação e/ou certificados instalados localmente na máquina do usuário, no padrão A1, bem como prover mecanismo de assinatura eletrônica avançada integrado à própria plataforma. Antes da efetivação da assinatura, o sistema deverá listar os certificados disponíveis para o usuário, permitindo a seleção do certificado desejado, exibindo apenas certificados vinculados ao próprio usuário. O sistema deverá indicar de forma clara quando um certificado estiver expirado, além de apresentar alerta caso o usuário já tenha realizado assinatura digital no mesmo documento, possibilitando a opção de cancelamento da nova assinatura.

No momento da solicitação ou realização da assinatura digital, o sistema deverá exibir o documento a ser assinado, quando se tratar de assinatura individual, ou permitir a visualização dos documentos relacionados, quando se tratar de assinatura em lote. Tal mecanismo visa garantir que o usuário tenha plena ciência do conteúdo e da natureza do documento que está assinando.

Todo documento PDF assinado digitalmente deverá conter estampa automática de verificação de autenticidade, incluindo informações para consulta pública do documento, com endereço eletrônico disponibilizado em formato de link e imagem de QR Code legível, permitindo a verificação por meio de leitura em dispositivos móveis (smartphones). O link deverá direcionar para uma página de validação da autenticidade do documento, contendo os detalhes do documento assinado, bem como a opção para download do arquivo assinado digitalmente.

ADEQUAÇÃO E ATENDIMENTO À LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)

Postulando alinhar a gestão da malha de informações cibernéticas às normativas punitivas da LGPD, os mecanismos a seguir serão ofertados na integralidade da plataforma:

- O arranjo propiciará um modelador exclusivo para redigir o documento de "Termos e Condições de Uso", focado tanto na vertente operacional do paço (repartições) quanto na população do portal externo. A liderança formatará o conteúdo legal conforme a adequação, variando-o por esferas de atendimento e segmentando por classes de acesso ao sistema;
- O coração do banco abrigará de forma descrita e permanente o "Inventário de Tratamentos de Dados Pessoais" incidentes em todas as rotinas automatizadas, explicitando ali de forma cristalina as fundamentações baseadas no ordenamento legal e nas justificativas atreladas aos usos sistêmicos;
- O Município terá o amparo para catalogar e injetar nesta relação outras instâncias analógicas ou atuações digitais em programas adjacentes, de modo a preservar no sistema da fornecedora um mapeamento total das coletas realizadas no cotidiano do serviço público;
- Um guichê inconfundível (Transparência Ativa) nascerá para iluminar de vez para o munícipe qual é o paradeiro e em que formatos o seu arcabouço informacional foi submetido a processamentos no paço (abarcando inclusive aquilo operado à margem do sistema contratado). Neste mesmo espaço, o contribuinte formalizará seus pedidos e pleiteará documentos de comprovação evidenciando seus rastros (Transparência Passiva);
- Disponibilizará impressão sumária listando os cruzamentos entre um CPF pesquisado e a estrutura do governo municipal (conferindo a clareza sobre os registros mantidos);
- Em conjunturas onde a aplicação do uso fuja do escopo da utilidade e segurança do amparo público incondicional, o cruzamento de referências forçará um atesto de anuência prévia assinalado ativamente pelo respectivo indivíduo titular das informações;
- Exigir espaço demarcado no painel da transparência para registrar e escancarar a nomenclatura, ramais de contato e identidade profissional do Agente Controlador e do Oficial de Proteção de Dados (DPO/Encarregado) definidos pela cúpula do paço;
- Diante da primeira entrada em solo digital (seja do morador ou do assessor administrativo), a tela reterá o trâmite até que o visitante leia as métricas de privacidade de consentimentos, abarcando o monitoramento local das interações (cookies). O veredito do usuário será carimbado nos relatórios ocultos de rastreio para chancelar posteriores exigências da procuradoria;
- A arquitetura abrirá serviço integrador (webservice) com o desígnio de chancelar que outras frentes digitais homologadas questionem, de forma remota, a validez ativa de anuência sobre tratamentos e compartilhamentos já averbados por algum titular e mapeados no seio do Município.

AUDITORIA, RASTREABILIDADE E CONTROLE DE ACESSOS

A solução deverá prover **múltiplas camadas de auditoria**, incluindo registros estruturados de eventos (logs) relativos às atividades executadas no ambiente sistêmico. Tais registros deverão contemplar, no mínimo:

- **Logs de operações de consulta**, registrando eventos de leitura de dados realizados pelos usuários nas diferentes rotinas do sistema;
- **Logs de operações de manipulação de dados (DML)** executadas sobre o banco de dados, abrangendo operações de **inclusão (INSERT), atualização (UPDATE) e exclusão (DELETE)**;
- **Logs de autenticação e controle de sessão**, registrando integralmente eventos de **login e logout**, incluindo metadados adicionais de segurança.

O sistema deverá permitir que o **administrador local da aplicação** gerencie os níveis de acesso às funcionalidades de auditoria, incluindo a capacidade de **conceder, restringir ou segmentar permissões de visualização e gerenciamento dos registros de auditoria** por perfis ou áreas funcionais do sistema.

Adicionalmente, o sistema deverá manter **registro permanente e imutável (audit trail)** de todas as operações de inclusão, alteração e exclusão realizadas nas tabelas da base de dados da aplicação, registrando obrigatoriamente os seguintes atributos:

- tipo de operação executada;
- identificação da rotina ou módulo da aplicação responsável pela operação;
- identificação da estação de trabalho de origem, mediante registro do **endereço IP da máquina cliente**;
- identificação inequívoca do usuário responsável pela operação;
- identificação da tabela afetada;
- classificação da operação executada (inclusão, alteração ou exclusão);
- conteúdo dos dados inseridos, modificados ou removidos.

Na interface de visualização dos registros de auditoria, o sistema deverá apresentar:

- **dados inseridos**, quando se tratar de operação de inclusão;
- **dados anteriores e novos valores**, quando se tratar de operação de alteração;
- **dados previamente existentes**, quando se tratar de operação de exclusão.

Monitoramento de Sessões e Administração de Usuários

O sistema deverá disponibilizar ao administrador funcional uma **interface administrativa integrada** que permita monitorar e gerenciar sessões ativas no servidor de aplicação. Essa interface deverá apresentar, no mínimo, as seguintes informações para cada sessão:

- data e hora de início da sessão;
- data e hora da última requisição efetuada ao servidor;
- código identificador da sessão;
- identificação e nome do usuário autenticado (quando aplicável);
- tempo total de duração da sessão;
- endereço IP da estação cliente.

Deverá também permitir ao administrador:

- **encerrar sessões ativas remotamente**;
- **enviar mensagens internas (notificações sistêmicas)** para um ou mais usuários autenticados na aplicação.

Histórico de Acessos

O sistema deverá manter **histórico detalhado de acessos**, registrando para cada operação executada:

- identificação do usuário;
- rotina ou funcionalidade acessada;
- ação executada;

- data e hora do evento;
- endereço IP da estação cliente no momento da execução.

Gerenciamento de Envio e Recebimento de E-mails

O sistema deverá disponibilizar **módulo centralizado de gerenciamento de comunicações por correio eletrônico**, contemplando, no mínimo, as seguintes funcionalidades:

- configuração de **múltiplas contas de e-mail** para envio e recebimento, centralizadas em um único módulo e compartilhadas entre os demais módulos do sistema;
- associação de **tipos de mensagens ou eventos do sistema** às contas de e-mail correspondentes;
- definição de **modelos padronizados de mensagens** para cada categoria de comunicação enviada;
- possibilidade de seleção manual da conta de e-mail no momento do envio da mensagem, entre aquelas previamente configuradas;
- capacidade de o administrador restringir ou permitir a alteração da conta de envio conforme o **tipo ou categoria da comunicação**.

O sistema deverá disponibilizar **monitoramento de envio de mensagens**, funcionando como uma **fila global de saída**, permitindo:

- acompanhamento do status de cada mensagem enviada;
- monitoramento das caixas de entrada das contas configuradas para identificação de **mensagens de retorno por falha (bounce)** provenientes do servidor ou dos destinatários;
- notificação automática ao usuário remetente sempre que for detectada falha na entrega da mensagem.

Gerenciamento e Emissão de Relatórios

O sistema deverá possuir **mecanismo robusto de geração e controle de relatórios**, contemplando as seguintes capacidades:

- execução simultânea de múltiplos relatórios pelo mesmo usuário;
- utilização de **fila de processamento de relatórios**, garantindo que a execução continue mesmo que o usuário finalize a sessão na aplicação;
- envio de **notificação automática ao usuário** após a conclusão do processamento do relatório;
- prevenção de execuções duplicadas de relatórios com **parâmetros idênticos** enquanto uma execução anterior ainda estiver em processamento;
- listagem de relatórios em processamento e relatórios concluídos.

Ao término da geração do relatório, o sistema deverá permitir:

- envio automático do relatório por e-mail para um ou mais destinatários cadastrados;
- definição de **agendamento de envio por data e hora específicas**.

O sistema deverá permitir a **assinatura digital de relatórios gerados**, bem como manter **cópia persistente de cada relatório emitido na base de dados**, associando cada emissão a um **identificador único (ID)**. Este identificador deverá ser impresso em todas as páginas do relatório juntamente com os seguintes metadados:

- filtros utilizados na geração;
- usuário responsável pela emissão;
- data e hora da emissão;
- identificador do relatório.

Adicionalmente, deverá existir **serviço de verificação de autenticidade no portal de serviços**, permitindo consultar e validar relatórios emitidos por meio do identificador único da emissão.

O sistema deverá permitir a consulta de relatórios previamente emitidos, aplicando filtros como:

- identificador da emissão;
- modelo ou layout do relatório;
- usuário emissor;
- data e hora da emissão.

A interface de consulta deverá exibir os parâmetros utilizados na geração e permitir nova impressão do documento.

Também deverá ser disponibilizado suporte para **impressão direta de documentos por dispositivos móveis**, incluindo smartphones ou tablets com sistema operacional Android, utilizando **impressoras térmicas com conectividade Bluetooth**. O fornecedor deverá informar os **requisitos mínimos de hardware e os equipamentos homologados**.

Gerador de Relatórios

O sistema deverá disponibilizar **ferramenta avançada de geração e customização de relatórios**, contendo, no mínimo, as seguintes funcionalidades:

- cadastro reutilizável de **formatos de relatório**, permitindo configuração de:
  - tamanho de página;
  - margens;
  - cabeçalho e rodapé;
  - brasão institucional;
  - numeração de páginas;
  - identificação da entidade;
  - filtros utilizados;
  - marca d'água configurável por upload de imagem.

A solução deverá permitir **edição avançada de layouts de relatórios**, contemplando:

- formatação de campos;
- inserção de imagens no corpo do relatório;
- definição de agrupamentos;
- geração de códigos de barras e **QR Code**.

A edição avançada poderá ser realizada por ferramenta externa, desde que **não implique custos adicionais para a contratante**.

O sistema deverá permitir:

- criação de novos layouts a partir de **cópia de layouts existentes**;
- seleção de dados por meio de **metadados da modelagem do sistema** ou através de **consultas SQL**;
- definição de características de campos como nome, tamanho e parâmetros de filtragem;
- acesso direto aos relatórios pelos menus dos módulos ou por **barra de acesso rápido**;
- definição de privilégios de acesso aos relatórios;
- gerenciamento de **versionamento de relatórios**, permitindo criação de novas versões sem impactar versões em produção;
- restauração de versões anteriores quando necessário.

Gerador de Consultas

O sistema deverá possuir **ferramenta de geração de consultas dinâmicas**, contemplando:

- definição de privilégios de acesso às consultas criadas;
- seleção de dados por metadados da estrutura do sistema ou via **instruções SQL**;
- definição de atributos de campos e opções de filtragem;
- acesso pelas interfaces dos módulos e pela barra de acesso rápido;
- configuração de **valores padrão (default)** para filtros, podendo ser definidos por constantes, parâmetros do sistema ou scripts SQL.

As consultas geradas deverão utilizar os mesmos recursos disponíveis nas consultas nativas do sistema, incluindo:

- preferências de visualização;
- filtros avançados e operadores;
- funcionalidades de impressão.

O sistema deverá permitir que o usuário **marque consultas como favoritas**, integrando-as ao menu personalizado do usuário.

Agendamento de Tarefas

O sistema deverá disponibilizar **mecanismo de agendamento de tarefas automatizadas**, contemplando:

- definição visual de fluxos de execução de atividades por meio de **modelagem gráfica similar a fluxogramas**;
- execução de ações automatizadas como:
  - geração de relatórios;
  - verificação de condições em registros da base de dados;
  - envio de notificações por e-mail.

Deverá permitir **agendamento recorrente**, incluindo execuções:

- diárias;
- mensais;
- anuais;
- em horários específicos.

Também deverá permitir a consulta do **histórico de execuções**, incluindo:

- status de execução;
- registros detalhados de logs.

Workflow e Gestão de Processos

O sistema deverá incorporar **mecanismo nativo de gerenciamento de fluxos de trabalho (Workflow)**, integrado ao mesmo ambiente de gestão e utilizando o **mesmo SGBD da aplicação**, sem necessidade de integração com sistemas externos.

A ferramenta deverá permitir:

- documentação de processos por meio de textos e associação de documentos digitais cadastrados;
- execução automatizada de funções do sistema e carregamento de formulários através de um **gerenciador centralizado**.

O módulo de workflow deverá permitir o **desenho de processos utilizando a notação BPMN (Business Process Model and Notation)**, incluindo elementos como:

- raias (lanes) horizontais e verticais;
- eventos;
- atividades;
- gateways e fluxos de processo.

Deverá permitir:

- controle de **ativação, desativação, homologação e versionamento de processos**;
- registro de histórico completo de alterações realizadas nos fluxos de trabalho;
- visualização comparativa entre versões;
- restauração de versões anteriores quando necessário.

Por fim, o sistema deverá também suportar **impressão direta de documentos por dispositivos móveis Android em impressoras térmicas Bluetooth**, devendo o fornecedor informar os **requisitos técnicos mínimos e a lista de equipamentos homologados** para operação adequada.