ANEXO III – ESPECIFICAÇÕES TÉCNICAS - APLICATIVO MÓVEL

PROCESSO ADMINISTRATIVO Nº 9034/2025

1. DESCRIÇÃO DA SOLUÇÃO (APLICATIVO MÓVEL DE RH)

1.1. O objeto inclui a disponibilização de aplicativo móvel de Recursos Humanos, compatível, no mínimo, com sistemas operacionais Android e iOS, destinado a dar mobilidade às principais rotinas de gestão de pessoas, permitindo que colaboradores e gestores realizem consultas e solicitações diretamente em smartphones e tablets, por meio de interface intuitiva e amigável.

1.2. O aplicativo deverá atender a instituições de diferentes portes e segmentos, garantindo alta capacidade de escala, sem prejuízo de desempenho e disponibilidade. A solução deverá ser ofertada preferencialmente em modelo SaaS (Software como Serviço), com licenciamento vinculado à quantidade de usuários/empregados, integrada, em tempo real, ao sistema de folha de pagamento e demais módulos de gestão de pessoas utilizados pelo órgão.

1.3. Todos os processos realizados no aplicativo deverão atualizar automaticamente a base de dados do sistema de RH/Folha, assegurando rastreabilidade das operações, integridade dos dados e histórico de registros. A solução deverá permitir parametrizações para adequação às políticas internas de pessoal e às características específicas da instituição, evitando a necessidade de desenvolvimentos sob medida para cada ajuste de regra de negócio.

2. BENEFÍCIOS ESPERADOS COM O APLICATIVO MÓVEL

2.1. A adoção do aplicativo móvel de RH visa à descentralização das rotinas operacionais de Recursos Humanos, reduzindo a circulação de documentos em papel, a burocracia e a dependência de atendimento presencial, com consequente redução de custos operacionais e aumento da eficiência da área. Espera-se ampliar a autonomia de colaboradores e gestores na execução das rotinas de RH, liberando a equipe de Recursos Humanos para atuação mais analítica e estratégica.

2.2. O aplicativo deverá contribuir para maior transparência na relação entre o órgão e seus colaboradores, por meio do acesso facilitado a informações funcionais, registros de jornada e documentos trabalhistas. A solução deverá estar em conformidade com a legislação trabalhista, incluindo funcionalidades de controle de jornada aderentes à Portaria 671/2021, quando aplicável, bem como observância às normas de proteção de dados pessoais.

3. REQUISITOS FUNCIONAIS MÍNIMOS DO APLICATIVO

3.1. O aplicativo móvel de Recursos Humanos deverá contemplar, no mínimo, as seguintes funcionalidades:

a) Consulta a envelope de pagamento (holerite) e informes de rendimento, diretamente em dispositivo móvel.

b) Registro e controle de batidas de ponto, inclusive em trabalho remoto, com recursos de biometria e geolocalização, em aderência à Portaria 671/2021, quando aplicável ao regime de trabalho do órgão.

c) Visualização do espelho de ponto pelo colaborador, observando os requisitos legais para apresentação das marcações e totalização de jornada.

d) Acesso ao banco de horas, com consulta a saldos individuais pelos colaboradores e visão consolidada pelo gestor da equipe.

e) Registro de solicitações pelos colaboradores, tais como: férias, abonos de ponto, envio de atestados médicos e demais ocorrências de rotina.

f) Aprovação de solicitações pelos gestores, individualmente ou em lote, incluindo férias, abonos e demais pedidos relacionados à equipe sob sua responsabilidade.

g) Consulta a histórico salarial, permitindo acompanhar evolução remuneratória, promoções e alterações de cargo, conforme perfis de acesso.

h) Disponibilização de dashboards de gestão para os gestores, com visão de férias programadas, pendências de aprovação e informações relevantes ao acompanhamento da equipe.

i) Recursos de apoio à gestão de férias, possibilitando a identificação de férias vencidas e próximas ao vencimento, visando ao cumprimento dos prazos legais.

j) Envio e recebimento de comunicados de RH por meio do aplicativo, com possibilidade de direcionamento a grupos específicos de colaboradores.

k) Envio de notificações push para eventos relevantes relacionados à gestão de pessoas (disponibilização de holerite, comunicados, pendências de aprovação, entre outros).

3.2. Quando contemplado no escopo da solução integrada de RH, o aplicativo poderá ainda incluir:

a) Fluxos de solicitação de alteração de dados funcionais, aumento de quadro, transferência e substituição de colaboradores, com tramitação para as áreas responsáveis.

b) Visualização de relatórios gerenciais predefinidos pelos gestores, observando perfis de acesso e segregação de funções.

c) Integração com solução de crédito consignado, para acesso a operações de empréstimo consignado atreladas à folha de pagamento.

d) Integração com solução de assinatura eletrônica, permitindo assinatura digital de documentos como recibos de férias, avisos de férias, espelho de ponto e outros documentos de RH definidos pelo órgão.

3.3. Requisitos de integração e aspectos técnicos:

3.3.1. O aplicativo móvel deverá possuir integração nativa e em tempo real com o sistema de gestão de pessoas e folha de pagamento adotado pelo órgão, bem como com demais soluções complementares eventualmente contratadas, tais como sistemas de ponto eletrônico, consignado e assinatura eletrônica. As integrações deverão garantir consistência dos dados, tratamento das regras de negócio de RH e segurança da informação, inclusive em ambiente de acesso remoto.

3.3.2. A solução deverá observar os requisitos legais aplicáveis ao registro de jornada eletrônica, em especial as disposições da Portaria 671/2021, no que couber, bem como as diretrizes de proteção de dados pessoais previstas na legislação vigente. O aplicativo deverá adotar boas práticas de segurança, autenticação e controle de acesso, alinhadas às políticas de segurança da informação do órgão.

3.4. Proteção de dados e privacidade:

3.4.1. A solução de software de gestão de pessoas e o aplicativo móvel de RH deverão observar integralmente a legislação aplicável à proteção de dados pessoais, em especial a Lei Geral de Proteção de Dados Pessoais – LGPD, adotando mecanismos que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. A contratada deverá implementar controles de acesso restrito, políticas de segurança da informação e medidas de proteção compatíveis com a natureza dos dados pessoais e sensíveis armazenados e processados no sistema.

3.4.2. Quando atuar na condição de operadora de dados pessoais, a fornecedora deverá cumprir as diretrizes contratuais estabelecidas pelo órgão contratante, bem como as normas legais e regulamentares vigentes, mantendo registro das operações de tratamento realizadas em nome do controlador. Quando atuar como fornecedora de software, a solução deverá disponibilizar recursos que auxiliem o órgão na governança de

dados pessoais, incluindo funcionalidades de configuração de perfis de acesso, registros de auditoria e demais controles necessários para atendimento à LGPD.

3.4.3. A solução deverá adotar metodologias e boas práticas de privacidade desde a concepção e por padrão (Privacy by Design e Privacy by Default), assegurando que novos produtos, serviços, integrações e evoluções contemplem requisitos de proteção de dados pessoais. Deverá, ainda, permitir a extração de informações necessárias ao exercício dos direitos dos titulares, tais como confirmação de tratamento, acesso, correção, anonimização, bloqueio ou eliminação de dados pessoais, nos termos da legislação vigente.

3.4.4. Nos casos em que houver compartilhamento de dados pessoais com terceiros (por exemplo, prestadores de serviços de consignado, assinatura eletrônica ou outros parceiros integrados), a solução deverá garantir que tal compartilhamento ocorra em conformidade com as bases legais aplicáveis e com as obrigações contratuais firmadas entre as partes. A contratada deverá, ainda, manter canal de comunicação para suporte ao órgão na resposta a demandas de titulares de dados e de autoridades competentes relacionadas ao tratamento realizado por meio da solução contratada.

4. REQUISITOS DE SEGURANÇA DO APLICATIVO MÓVEL

4.1. Escopo e Princípios Gerais

4.1.1. O aplicativo móvel integra o escopo da solução contratada e deverá atender integralmente aos requisitos de segurança da informação, privacidade e proteção de dados definidos nesta especificação técnica, inclusive os requisitos gerais de segurança.

4.2. Restrições de Acesso Administrativo

4.2.1. É vedado o acesso a funcionalidades administrativas da solução por meio do aplicativo móvel, incluindo, mas não se limitando a:

a) Criação, exclusão ou alteração de usuários;

b) Gestão de perfis, papéis, permissões ou políticas de acesso;

c) Parametrizações globais do sistema;

d) Administração de segurança, autenticação, autorização ou integrações;

e) Acesso irrestrito a dados classificados como sensíveis ou críticos.

4.2.2. As funcionalidades administrativas deverão ser exclusivamente acessíveis por interface web, em ambiente controlado, mediante autenticação forte e controles adicionais de segurança.

4.2.3. Usuários que possuam perfil administrativo na plataforma web, ao acessarem o aplicativo móvel, deverão ter seu escopo funcional automaticamente restrito às funcionalidades permitidas para empregados, conforme regras de autorização definidas.

4.2.4. É vedada qualquer forma de elevação de privilégio via aplicativo móvel, ainda que o usuário possua credenciais administrativas válidas no ambiente web.

4.2.5. Tentativas de acesso a funcionalidades administrativas por meio do aplicativo móvel deverão:

a) Ser bloqueadas automaticamente;

b) Ser registradas em log de segurança;

c) Gerar alerta para fins de monitoramento e auditoria.

4.3. Autenticação, Sessão e Controle de Acesso

4.3.1. O gerenciamento de sessão deverá contemplar, no mínimo:

a) Expiração automática por inatividade;

b) Revogação remota de sessões ativas;

c) Limitação e bloqueio após tentativas inválidas consecutivas;

d) Proteção contra reutilização de sessão.

4.3.2. O aplicativo não deverá permitir compartilhamento de sessão entre usuários, ainda que no mesmo dispositivo.

4.4. Proteção de Dados no Dispositivo

4.4.1. É vedado o armazenamento de credenciais, tokens, dados pessoais, dados sensíveis, dados biométricos ou informações funcionais em texto claro no dispositivo móvel.

4.4.2. Quando tecnicamente necessário o armazenamento local de dados, este deverá:

a) Utilizar criptografia forte em repouso (AES-256 ou superior);

b) b. Utilizar mecanismos nativos de proteção do sistema operacional (Keychain, Keystore ou equivalente);

c) Restringir-se às informações estritamente necessárias à funcionalidade.

4.4.3. O aplicativo deverá implementar mecanismos para eliminação segura dos dados armazenados localmente em caso de logout, revogação de acesso ou desinstalação.

4.4.4. Os dados armazenados localmente deverão observar retenção mínima necessária à funcionalidade, sem exposição integral em notificações push, pré-visualização de tela bloqueada ou outros mecanismos que possam revelar conteúdo sensível a terceiros.

4.5. Comunicação Segura

4.5.1. Toda comunicação entre o aplicativo móvel e os serviços backend deverá ocorrer exclusivamente por meio de canais criptografados, utilizando TLS versão 1.3 ou superior.

4.5.2. O aplicativo deverá implementar validação de certificados para mitigação de ataques do tipo Man-in-the-Middle.

4.5.3. É vedado o uso de protocolos, algoritmos ou bibliotecas criptográficas obsoletas ou consideradas inseguras, durante todo o tempo de vida da solução.

4.5.4. O aplicativo deverá adotar pinning de certificado ou mecanismo equivalente de confiança, quando tecnicamente viável, para reduzir o risco de interceptação de tráfego.

4.5.5. O aplicativo deverá empregar mecanismos de proteção contra adulteração, reempacotamento, engenharia reversa e injeção de código, inclusive com verificação de integridade em tempo de execução, quando aplicável.

4.6. Segurança do Ambiente e do Dispositivo

4.6.1. O aplicativo deverá possuir mecanismos para detecção de ambientes comprometidos, incluindo, no mínimo:

a) Dispositivos com root ou jailbreak;

b) Emuladores não autorizados;

c) Execução com debug ativo em ambiente produtivo.

4.6.2. A CONTRATANTE poderá definir políticas de restrição ou bloqueio de uso do aplicativo em dispositivos que não atendam aos requisitos mínimos de segurança.

4.7. Atualizações, Vulnerabilidades e Testes

4.7.1. A CONTRATADA deverá manter o aplicativo móvel compatível com as versões mais recentes dos sistemas operacionais Android e iOS durante toda a vigência do contrato.

4.7.2. Vulnerabilidades identificadas no aplicativo móvel deverão ser tratadas conforme sua criticidade.

4.7.3. O aplicativo móvel deverá ser submetido periodicamente:
a) Análise estática (SAST) e dinâmica (DAST) de código (no fluxo/pipeline de desenvolvimento);

b)Testes de segurança em aplicações móveis (no mínimo uma vez ao ano e com comprovação de execução e correções enviadas a CONTRATANTE).

4.7.4. As vulnerabilidades deverão possuir prazos máximos de correção compatíveis com sua criticidade, a serem definidos em acordo de nível de serviço.

4.7.5. A CONTRATADA deverá informar à CONTRATANTE as correções aplicadas, os componentes afetados e o resultado dos testes de validação após cada atualização de segurança.

4.8. Distribuição, Integridade e Atualizações

4.8.1. O aplicativo móvel deverá ser distribuído exclusivamente por lojas oficiais (minimamente Android Play Store e Apple App Store).

4.8.2. A CONTRATADA deverá adotar mecanismos que garantam a integridade do aplicativo, prevenindo adulteração, reempacotamento ou distribuição não autorizada.

4.8.3. Atualizações do aplicativo não poderão reduzir ou remover controles de segurança previamente implementados.