

## CHECKLIST PARA CONSTRUÇÃO DE UM BACKEND DE SAAS

### AUTENTICAÇÃO & AUTORIZAÇÃO

- ☐ Cadastro de usuário
- ☐ Login
- ☐ Logout / Invalidação de token
- ☐ Recuperação de senha
- ☐ Reenvio de confirmação (opcional)
- ☐ Verificação de email
- ☐ Atualizar senha
- ☐ Atualizar email
- ☐ Autenticação JWT / Session
- ☐ 2FA (opcional)
- ☐ Middleware de rotas protegidas

### PERFIL DO USUÁRIO

- ☐ Editar nome, avatar e dados pessoais
- ☐ Alterar senha
- ☐ Alterar email
- ☐ Desativar conta
- ☐ Histórico mínimo de atividades (opcional)

### ORGANIZAÇÕES / TIMES (MULTI-TENANT)

- ☐ Criar organização
- ☐ Convidar usuários para organização
- ☐ Aceitar convite
- ☐ Remover usuário da organização
- ☐ Transferir propriedade da organização
- ☐ Listar membros
- ☐ Trocar organização ativa

- [ ] Middleware para isolar dados por tenant

#### PERMISSÕES (RBAC/ACL)

- [ ] Definição de roles
- [ ] Permissões baseadas em roles
- [ ] Permissões em recursos (ACL opcional)
- [ ] Middleware de autorização granular

#### PLANOS & ASSINATURAS

- [ ] Criar planos
- [ ] Criar assinatura
- [ ] Cancelar assinatura
- [ ] Renovação automática
- [ ] Trial gratuito
- [ ] Verificação de limites por plano
- [ ] Middleware para verificar plano/limites
- [ ] Webhooks do gateway de pagamento
- [ ] Tratamento de falhas de pagamento

#### BILLING & FINANCEIRO

- [ ] Histórico de cobranças
- [ ] Detalhes da assinatura atual
- [ ] Notificação de cobrança falhada
- [ ] Atualizar dados de cobrança
- [ ] Exportar dados financeiros (opcional)

#### EMAILS & NOTIFICAÇÕES

- [ ] Templates de email
- [ ] Envio de emails transacionais
- [ ] Notificações internas
- [ ] Emails em eventos importantes

## ARMAZENAMENTO & UPLOADS

- ☐ Upload seguro de arquivos
- ☐ Validação de tamanho e tipo
- ☐ Armazenamento externo (S3 etc.)
- ☐ Controle de acesso a arquivos por tenant
- ☐ Limite de armazenamento por plano

## AUDITORIA, LOGS & MONITORAMENTO

- ☐ Logs de atividade
- ☐ Logs de erros
- ☐ Rate limiting
- ☐ Monitoramento
- ☐ Registro de auditoria

## API & INTEGRAÇÕES

- ☐ API REST
- ☐ Documentação Swagger
- ☐ Versionamento
- ☐ Tokens pessoais
- ☐ Webhooks
- ☐ Filtros & paginação

## INFRAESTRUTURA MULTI-TENANT

- ☐ Modelo escolhido
- ☐ Middleware para detectar tenant
- ☐ Uso obrigatório de tenantId
- ☐ Isolamento de dados validado
- ☐ Estratégia de backup por tenant

## PAINEL ADMIN

- ☐ Usuários

- [ ] Organizações

- [ ] Assinaturas

- [ ] Planos

- [ ] Logs

- [ ] Estatísticas

## SEGURANÇA

- [ ] Hash forte de senha

- [ ] Validação de entrada

- [ ] CORS

- [ ] Rate limit global

- [ ] CSRF (se session)

- [ ] Sanitização de input

- [ ] Anti-fraude em pagamentos

## FINALIZAÇÃO

- [ ] Backup automático

- [ ] Restore testado

- [ ] Documentação

- [ ] Seeders

- [ ] Ambiente de homologação

- [ ] CI/CD