🔐 Sistema de Permissões RBAC

Nexus Atemporal - CRM para Clínicas de Estética

Versão 1.0 - Outubro 2025

📋 Índice

1. Hierarquia de Usuários
2. Matriz de Permissões Detalhada
3. Tabela Comparativa Resumida
4. Estrutura Técnica
5. Implementação no Código

🎭 1. Hierarquia de Usuários

🔱 SUPERADMIN (Nexus Atemporal)

↓

👑 OWNER (Dono da Clínica)

↓

⚡ ADMIN (Gerente/Coordenador)

↓

👤 USER (Recepcionista/Atendente)

↓

🩺 PROFESSIONAL (Médico/Esteticista)

🔐 2. Matriz de Permissões Detalhada

🔱 SUPERADMIN

Acesso total ao sistema, todos os tenants

✅ Permissões:

- ✅ Acessar qualquer tenant/clínica
- ✅ Criar/editar/excluir tenants
- ✅ Gerenciar planos e billing de todos
- ✅ Acessar logs de todos os sistemas
- ✅ Configurar integrações globais (n8n, Typebot, Waha)
- ✅ Modificar código/infraestrutura
- ✅ Ver métricas consolidadas de todos os clientes
- ✅ Suporte técnico avançado
- ✅ Acesso ao banco de dados
- ✅ Gerenciar superadmins

> ***Casos de uso:*** *Você, equipe de desenvolvimento, suporte nível 3*

👑 OWNER

Controle total do seu tenant/clínica

✅ Módulo Config/Configurações:

- ✅ Gerenciar plano e billing da clínica
- ✅ Upgrade/downgrade de plano
- ✅ Configurar gateways de pagamento
- ✅ Gerenciar integrações (WhatsApp, Google, etc)
- ✅ Configurar automações (n8n, Typebot)
- ✅ White label (logo, cores, domínio)
- ✅ Backup e exportação de dados
- ✅ Ver todos os logs de auditoria
- ✅ Configurações de segurança (2FA obrigatório, etc)

✅ Módulo Usuários:

- ✅ Criar/editar/excluir qualquer usuário
- ✅ Alterar roles de qualquer usuário
- ✅ Ver logs de atividade de todos
- ✅ Bloquear/desbloquear usuários
- ✅ Redefinir senhas de qualquer usuário

✅ Módulo Financeiro:

- ✅ Ver todos os dados financeiros
- ✅ Aprovar/reprovar pagamentos
- ✅ Configurar formas de pagamento

✅ Acessar relatórios fiscais completos

✅ Definir metas e comissões

✅ Ver lucro/prejuízo real

✅ Módulo BI/Analytics:

✅ Acessar todos os dashboards

✅ Ver métricas sensíveis (lucro, margem, CAC, LTV)

✅ Exportar todos os relatórios

✅ Usar IA para análises avançadas

✅ Todos os outros módulos:

✅ Acesso total de leitura e escrita

❌ Não pode:

❌ Acessar outros tenants

❌ Modificar configurações do superadmin

❌ Ver código-fonte ou infraestrutura

> ***Casos de uso:*** *Proprietário da clínica, sócio majoritário*

⚡ ADMIN

Gestão operacional da clínica

✅ Módulo Dashboard:

- ✅ Ver KPIs operacionais
- ✅ Ver alertas e notificações
- ⚠️ Ver métricas financeiras resumidas (sem detalhes de lucro)

✅ Módulo Leads:

- ✅ Criar/editar/excluir leads
- ✅ Atribuir leads para equipe
- ✅ Ver pipeline completo
- ✅ Usar qualificação automática
- ✅ Configurar funis e etapas
- ✅ Exportar relatórios de leads

✅ Módulo Agenda:

- ✅ Ver agenda de todos os profissionais
- ✅ Criar/editar/cancelar agendamentos de qualquer profissional
- ✅ Configurar horários de atendimento
- ✅ Gerenciar salas/recursos
- ✅ Sincronização Google Calendar (todos)

✅ Módulo Prontuários:

- ✅ Ver todos os prontuários

✅ Criar/editar prontuários

✅ Assinar digitalmente

✅ Anexar documentos

⚠️ Não pode excluir prontuários

✅ Módulo Financeiro:

✅ Lançar receitas e despesas

✅ Controlar caixa

✅ Gerar boletos/cobranças

✅ Ver contas a pagar/receber

⚠️ Ver relatórios gerenciais (sem margem de lucro detalhada)

❌ Aprovar pagamentos acima de R$ 5.000

❌ Alterar configurações de gateway

❌ Ver dados bancários completos

✅ Módulo Usuários:

✅ Ver lista de usuários

✅ Criar usuários USER e PROFESSIONAL

⚠️ Não pode criar ADMIN ou OWNER

⚠️ Não pode editar/excluir ADMIN ou OWNER

✅ Editar usuários USER e PROFESSIONAL

❌ Não pode:

❌ Excluir dados críticos (prontuários, transações antigas)

❌ Alterar plano/billing

❌ Configurar gateways de pagamento

❌ Ver logs de auditoria completos

❌ Acessar configurações de segurança avançadas

> ***Casos de uso:*** *Gerente de clínica, coordenador, supervisor*

👤 USER

Operação do dia a dia

✅ Módulo Leads:

✅ Ver leads atribuídos a si

✅ Criar novos leads

✅ Editar leads próprios

⚠️ Ver pipeline geral (somente leitura)

❌ Excluir leads

❌ Atribuir leads para outros

✅ Módulo Agenda:

👁️ Ver agenda de todos (somente leitura)

✅ Criar agendamentos

✅ Editar agendamentos criados por si

✅ Confirmar/cancelar agendamentos

⚠️ Não pode alterar horários dos profissionais

❌ Não pode configurar sincronização

✅ Módulo Financeiro:

✅ Registrar recebimentos simples

✅ Emitir boletos/cobranças

✅ Ver contas a receber do dia

❌ Ver relatórios financeiros

❌ Aprovar pagamentos

❌ Lançar despesas

❌ Controlar caixa (fechamento)

✅ Módulo Prontuários:

👁️ Visualizar prontuários (leitura)

⚠️ Criar fichas de anamnese básica

❌ Editar prontuários existentes

❌ Assinar prontuários

❌ Anexar documentos sensíveis

❌ Não pode:

❌ Acessar dados financeiros sensíveis

❌ Gerenciar usuários

❌ Configurar qualquer integração

❌ Exportar dados em massa

❌ Usar IA avançada

❌ Ver relatórios estratégicos

> ***Casos de uso:*** *Recepcionista, secretária, atendente*

🩺 PROFESSIONAL

Foco clínico, sem gestão

✅ Módulo Dashboard:

✅ Ver seu dashboard pessoal

✅ Ver suas métricas (atendimentos, avaliações, etc)

✅ Módulo Agenda:

✅ Ver SOMENTE sua própria agenda

✅ Bloquear horários pessoais

✅ Marcar ausências

⚠️ Não pode criar agendamentos para outros

❌ Não pode alterar configurações de agenda

✅ Módulo Prontuários (ACESSO TOTAL):

✅ Ver prontuários dos seus pacientes

✅ Criar e editar prontuários

✅ Assinar digitalmente

✅ Anexar fotos antes/depois

✅ Prescrever tratamentos

✅ Usar IA clínica (se disponível no plano)

✅ Exportar prontuários (PDF)

⚠️ Não pode excluir prontuários antigos (> 30 dias)

✅ Módulo Financeiro:

✅ Ver suas comissões

✅ Ver relatório de recebíveis próprios

❌ Não pode lançar receitas/despesas

❌ Não vê dados financeiros da clínica

❌ Não pode:

❌ Acessar dados de outros profissionais

❌ Gerenciar leads ou marketing

❌ Ver dados financeiros da clínica

❌ Configurar integrações

❌ Gerenciar usuários

> ***Casos de uso:*** *Médico, dentista, esteticista, fisioterapeuta*

📊 3. Tabela Comparativa Resumida

Módulo	SUPERADMIN	OWNER	ADMIN	USER	PROFESSIONAL
Dashboard	✅ Tudo	✅ Tudo	✅ Operacional	⚠️ Básico	⚠️ Pessoal
Leads	✅ Tudo	✅ Tudo	✅ Tudo	⚠️ Limitado	👁️ Leitura
Agenda	✅ Tudo	✅ Tudo	✅ Tudo	⚠️ Criar	⚠️ Só sua
Chat/WhatsApp	✅ Tudo	✅ Tudo	✅ Tudo	⚠️ Suas filas	⚠️ Seus pacientes
Prontuários	✅ Tudo	✅ Tudo	✅ Exceto excluir	👁️ Leitura	✅ Seus pacientes
Financeiro	✅ Tudo	✅ Tudo	⚠️ Sem lucro	⚠️ Receber	⚠️ Comissões
Estoque	✅ Tudo	✅ Tudo	✅ Tudo	👁️ Leitura + Saída	👁️ Leitura
BI/Analytics	✅ Tudo	✅ Tudo	⚠️ Operacional	❌ Não	⚠️ Pessoal
Marketing	✅ Tudo	✅ Tudo	✅ Tudo	❌ Não	❌ Não
Usuários	✅ Tudo	✅ Tudo	⚠️ USER/PROF	👁️ Leitura	👁️ Leitura
Configurações	✅ Tudo	✅ Tudo	👁️ Leitura	⚠️ Seu perfil	⚠️ Seu perfil
Billing/Planos	✅ Tudo	✅ Tudo	❌ Não	❌ Não	❌ Não

Legenda:

✅ Acesso completo

⚠️ Acesso parcial/limitado

👁️ Somente leitura

❌ Sem acesso

💻 4. Estrutura Técnica

4.1 Enum de Roles

```
export enum UserRole { SUPERADMIN = 'SUPERADMIN', OWNER = 'OWNER', ADMIN = 'ADMIN', USER = 'USER', PROFESSIONAL = 'PROFESSIONAL' }
```

4.2 Enum de Permissions

```
export enum Permission { // Leads LEADS_CREATE = 'leads.create', LEADS_READ = 'leads.read', LEADS_UPDATE = 'leads.update', LEADS_DELETE = 'leads.delete', LEADS_ASSIGN = 'leads.assign', // Financeiro FINANCIAL_VIEW_ALL = 'financial.view_all', FINANCIAL_VIEW_SUMMARY = 'financial.view_summary', FINANCIAL_CREATE = 'financial.create', FINANCIAL_APPROVE = 'financial.approve', // Prontuários RECORDS_VIEW_ALL = 'records.view_all', RECORDS_VIEW_OWN = 'records.view_own', RECORDS_CREATE = 'records.create', RECORDS_UPDATE = 'records.update', RECORDS_DELETE = 'records.delete', RECORDS_SIGN = 'records.sign', // ... mais permissões }
```

4.3 Schema do Banco de Dados

```
CREATE TYPE user_role AS ENUM ( 'SUPERADMIN', 'OWNER', 'ADMIN', 'USER', 'PROFESSIONAL' ); CREATE TABLE users ( id UUID PRIMARY KEY, tenant_id UUID REFERENCES tenants(id), email VARCHAR(255) UNIQUE NOT NULL, name VARCHAR(255) NOT NULL, role user_role NOT NULL DEFAULT 'USER', is_active BOOLEAN DEFAULT true, created_at TIMESTAMP DEFAULT NOW() ); CREATE TABLE permissions ( id UUID PRIMARY KEY, name VARCHAR(100) UNIQUE NOT NULL, description TEXT, module VARCHAR(50) NOT NULL, action VARCHAR(50) NOT NULL ); CREATE TABLE role_permissions ( id UUID PRIMARY KEY, role user_role NOT NULL, permission_id UUID REFERENCES permissions(id), UNIQUE(role, permission_id) );
```

🔧 5. Implementação no Código

5.1 Middleware de Autorização

```
// backend/src/shared/middlewares/authorize.middleware.ts export const authorize = (...requiredPermissions: Permission[]) => { return (req: Request, res: Response, next: NextFunction) => { const user = req.user; if (!user) { return res.status(401).json({ message: 'Não autenticado' }); } // Superadmin sempre passa if (user.role === UserRole.SUPERADMIN) { return next(); } const userPermissions = ROLE_PERMISSIONS[user.role] || []; const hasPermission = requiredPermissions.every(p => userPermissions.includes(p) ); if (!hasPermission) { return res.status(403).json({ message: 'Sem permissão', required: requiredPermissions }); } next(); }; };
```

5.2 Uso nas Rotas

```
// Criar lead - USER, ADMIN, OWNER podem router.post( '/leads', authenticate, authorize(Permission.LEADS_CREATE), leadsController.create ); // Excluir lead - apenas ADMIN e OWNER router.delete( '/leads/:id', authenticate, authorize(Permission.LEADS_DELETE), leadsController.delete ); // Configurar billing - apenas OWNER router.post( '/config/billing', authenticate, requireRole(UserRole.OWNER), configController.updateBilling );
```

5.3 Hook React de Permissões

```
// frontend/src/hooks/usePermissions.ts export const usePermissions = () => { const { user } = useAuthStore(); const can = { createLead: () => hasPermission('leads.create'), deleteLead: () => hasPermission('leads.delete'), viewFinancial: () => hasPermission('financial.view_all'), manageBilling: () => hasPermission('config.billing'), }; return { can, hasRole, user }; }; // Uso no componente: const { can } = usePermissions(); {can.deleteLead() && ( Excluir )}
```

5.4 Componente de Proteção

```
// Proteger componentes por permissão <Protected
permission="leads.delete"> <button>Excluir Lead</button> </Protected> //
Proteger por role <Protected role={['OWNER', 'ADMIN']}>
<FinancialDashboard /> </Protected>
```

📝 Notas Importantes

🔒 Segurança

- Sempre validar permissões no backend, nunca confiar apenas no frontend
- SUPERADMIN tem acesso a TUDO, use com cuidado
- Logs de auditoria devem registrar todas as ações sensíveis
- Implementar rate limiting para prevenir abuso

🎯 Boas Práticas

- Sempre usar princípio do menor privilégio
- Revisar permissões periodicamente
- Documentar mudanças no sistema de permissões
- Testar fluxos de cada role antes de deploy

🚀 Próximos Passos

- Implementar migrations do banco de dados
- Criar seeds com permissões padrão
- Desenvolver tela de gerenciamento de usuários
- Implementar logs de auditoria
- Criar testes automatizados para cada role

Nexus Atemporal - Sistema de Gestão para Clínicas

Documentação versão 1.0 - Outubro 2025

contato@nexusatemporal.com.br