

|  |
| --- |
| **Sistema IA – Portal Web**  Documento de Requisitos  (Submódulo Permissões) |
|  |
| Versão 1.0 |

|  |
| --- |
| Clovis Ap. Moratta  17/9/2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| **HISTÓRICO DE REVISÕES** | | | |
| Data | Versão | Descrição | Autor |
| 17/09/2025 | 1.0 | Criação do documento de requisitos “Submódulo Permissões” | Clovis Ap. Moratta |
|  |  |  |  |
|  |  |  |  |

**SUMÁRIO**

[1) Informações do Projeto 3](#_Toc209021628)

[2. Objetivo e Escopo 3](#_Toc209021629)

[3. Atores e Permissões 3](#_Toc209021630)

[4. Visão Geral Funcional 3](#_Toc209021631)

[5. Requisitos Funcionais (RF) 4](#_Toc209021632)

[6. Requisitos Não Funcionais (RNF) 4](#_Toc209021633)

[7. Regras de Negócio e Invariantes 4](#_Toc209021634)

[8. Casos de Uso (Descritivo) 5](#_Toc209021635)

[**Caso de Uso UC01:** Cadastrar Módulo 5](#_Toc209021636)

[**Caso de Uso UC02:** Cadastrar Submódulo 5](#_Toc209021637)

[**Caso de Uso UC03:** Editar/Excluir Módulo 6](#_Toc209021638)

[**Caso de Uso UC04:** Editar/Excluir Submódulo 6](#_Toc209021639)

[**Caso de Uso UC05:** Manter Matriz de Permissões 7](#_Toc209021640)

[**Caso de Uso UC06**: Autorizar Ação (consumo FE/BE) 7](#_Toc209021641)

[**Caso de Uso UC07:** Sincronizar Catálogo (Seed/Sync) 8](#_Toc209021642)

[**Caso de Uso UC08:** Copiar/Importar/Exportar (opcional) 8](#_Toc209021643)

[9. Interface do Usuário (referência) 9](#_Toc209021644)

[10. Dados e Integrações 10](#_Toc209021645)

[11. Mensagens do Sistema 10](#_Toc209021646)

[12. Considerações de LGPD e Segurança 10](#_Toc209021647)

[13. Estrutura de Dados (Proposta) 10](#_Toc209021648)

[14. Referências do Projeto 11](#_Toc209021649)

[15. Mapa de Integrações 11](#_Toc209021650)

[16. Integração com o Projeto Existente (Resumo) 12](#_Toc209021651)

# 1) Informações do Projeto

* **Projeto:** IA - Portal Web - Protótipo
* **Módulo:** Segurança
* **Submódulo:** Permissões

**Descrição:** Cadastro de módulos e submódulos e definição de permissões (Acesso, Incluir, Editar, Visualizar, Excluir) por Grupo. Validação obrigatória de permissões em todos os submódulos do sistema.

# 2. Objetivo e Escopo

**Objetivo**

Disponibilizar CRUD de Módulos/Submódulos e matriz de permissões por Grupo; fornecer endpoints/contratos para verificação de autorização no Front-End/Back-End; garantir validação obrigatória de permissões em todo o sistema.

**Escopo – Incluído**

* Manter Módulos e Submódulos (codes canônicos)
* Matriz de permissões por Grupo (Acesso, Incluir, Editar, Visualizar, Excluir)
* Endpoints de autorização (pontual e cache)
* Seed/Sync do catálogo a partir do menu/manifesto
* Copiar/Importar/Exportar permissões (opcional)
* Aplicação das permissões em \*\*todos\*\* os submódulos existentes (Usuários, Grupos, Grupos X Usuários, Logs de Acesso, Chamados).

**Escopo – Excluído**

* Cadastro/edição de Usuários
* Associação Usuários↔Grupos
* Relatórios analíticos de Logs de Acesso

# 3. Atores e Permissões

**Ator Principal:** Administrador do Sistema (permissão: gerenciar associações de usuários a grupos).

**Permissões do ator:** Gerenciar Módulos/Submódulos; editar permissões; executar sync/importação/exportação.

# 4. Visão Geral Funcional

Tela em dois painéis: árvore (Módulos/Submódulos) à esquerda e matriz de permissões (Grupos x flags) à direita; ações via modais. Validação obrigatória de permissões através de guards (Front-end) e policies/decorators (Back-end) consumindo as regras deste submódulo.

# 5. Requisitos Funcionais (RF)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Título** | **Descrição** | **Critérios de Aceite** |
| RF01 | Manter Módulos | CRUD de módulos com module\_code único. | Validar nome e code; impedir exclusão com submódulos/permissões; auditoria; IN02/IN03/IN04. |
| RF02 | Manter Submódulos | CRUD de submódulos vinculados a módulo. | Unicidade de submodule\_code por módulo; impedir exclusão com permissões; auditoria; IN05/IN06/IN07. |
| RF03 | Matriz de Permissões | Exibir/editar permissões por grupo. | Flags access/create/edit/view/delete; 'access' pré-requisito; submódulo prevalece; salvar em lote/linha; IN08/IN09. |
| RF04 | Autorizar Ação (API) | Endpoints para verificação FE/BE. | POST /api/auth/authorize retorna {allowed}; GET /api/auth/me/permissions para cache; P95 authorize ≤50ms; 403 padronizado. |
| RF05 | Sincronizar Catálogo | Seed/sync de módulos/submódulos a partir do menu/manifesto. | Sem duplicar; atualizar codes; relatório de alterações; IN12. |
| RF06 | Copiar Permissões (opcional) | Copiar permissões entre grupos. | Selecionar origem/destinos; confirmação; auditoria; IN10. |
| RF07 | Importar/Exportar (opcional) | Permissões via CSV/JSON. | Validação de schema; preview; atomicidade por lote; IN11. |
| RF08 | Validação obrigatória de permissões | Obrigar uso de permissões em todos os submódulos. | Front-end: guards/ocultação de ações; Back-end: decorators/policies; 403 padronizado; evidências em PRs. |

# 6. Requisitos Não Funcionais (RNF)

|  |  |  |
| --- | --- | --- |
| **ID** | **Categoria** | **Requisito** |
| RNF01 | Performance | P95 ≤ 3000 ms em listar/editar; authorize P95 ≤ 50 ms com cache |
| RNF02 | Disponibilidade | Meta ≥ 99,5% mensal para o serviço de consulta. |
| RNF03 | Usabilidade | UI consistente; validações claras; mensagens padrão |
| RNF04 | Segurança | Restrição de acesso; logs de auditoria; autenticação e autorização centralizadas. |

# 7. Regras de Negócio e Invariantes

|  |  |  |
| --- | --- | --- |
| **ID da Regra (RN)** | **Descrição** | **Aplica a** |
| RN01 | module\_code e submodule\_code obrigatórios e imutáveis; nome é rótulo. | RF01, RF02 |
| RN02 | Unicidade: module\_code global; submodule\_code único por módulo. | RF01, RF02 |
| RN03 | 'access=true' é pré-requisito para create/edit/view/delete. | RF03 |
| RN04 | Permissão no submódulo prevalece sobre a do módulo. | RF03 |
| RN05 | Todos os endpoints/telas de negócio devem validar permissão (policy/guard). | RF08 |
| RN06 | Catálogo deve ser sincronizado com menu/manifesto. | RF05 |
| RN07 | Auditoria completa (quem, quando, antes/depois) nas operações relevantes. | RF01..RF08 |

# 8. Casos de Uso (Descritivo)

## **Caso de Uso UC01:** Cadastrar Módulo

**Descrição:** Criar módulo com module\_code e nome exibido.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado com permissão de criar módulos.

• **Fluxo Principal:**

1. Abrir modal 'Novo Módulo'.
2. Preencher nome, module\_code, descrição, ativo.
3. Confirmar criação.
4. Sistema salva e atualiza árvore.

• **Fluxo Alternativo:**

1. module\_code duplicado → erro.
2. Falha API → mensagem de erro.

• **Pós-condições:** Módulo cadastrado e auditado.

• **Integração:** IN02 — POST /api/seguranca/modulos

## **Caso de Uso UC02:** Cadastrar Submódulo

Descrição: Criar submódulo vinculado ao módulo.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado.
2. Módulo existente selecionado.

• **Fluxo Principal:**

1. Abrir modal 'Novo Submódulo'.
2. Preencher submodule\_code, nome, rota, ativo.
3. Confirmar.
4. Sistema salva e atualiza árvore.

• **Fluxo Alternativo:**

1. Duplicidade de submodule\_code por módulo → erro.
2. Falha API → erro.

• **Pós-condições:** Submódulo cadastrado e auditado.

• **Integração:** IN05 — POST /api/seguranca/submodulos

## **Caso de Uso UC03:** Editar/Excluir Módulo

**Descrição:** Editar dados ou excluir módulo, respeitando vínculos.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado.
2. Módulo existente.

• **Fluxo Principal:**

1. Abrir modal Editar/Excluir.
2. Atualizar campos ou confirmar exclusão.
3. Sistema valida vínculos (submódulos/permissões) e salva.

• **Fluxo Alternativo:**

1. Bloqueado por vínculos → erro orientativo.
2. Falha API → erro.

• **Pós-condições:** Módulo atualizado/excluído; auditoria registrada.

• **Integração:** IN03 — PUT/PATCH /api/seguranca/modulos/{id}; IN04 — DELETE /api/seguranca/modulos/{id}

## **Caso de Uso UC04:** Editar/Excluir Submódulo

**Descrição:** Editar dados ou excluir submódulo, respeitando vínculos.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado.
2. Submódulo existente.

• **Fluxo Principal:**

1. Abrir modal Editar/Excluir.
2. Atualizar campos ou confirmar exclusão.
3. Sistema valida vínculos (permissões) e salva.

**• Fluxo Alternativo:**

1. Bloqueado por vínculos → erro orientativo.
2. Falha API → erro.

• **Pós-condições:** Submódulo atualizado/excluído; auditoria registrada.

• **Integração:** IN06 — PUT/PATCH /api/seguranca/submodulos/{id}; IN07 — DELETE /api/seguranca/submodulos/{id}

## **Caso de Uso UC05:** Manter Matriz de Permissões

**Descrição:** Ajustar permissões de grupos para módulo/submódulo.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado.
2. Módulo/Submódulo selecionado.
3. Grupos existentes cadastrados.

• **Fluxo Principal:**

1. Marcar/desmarcar checkboxes por linha.
2. Clicar 'Salvar' (lote/linha).
3. Sistema valida dependências (access) e prevalência (submódulo>módulo) e salva.

• **Fluxo Alternativo:**

1. Violação de regra (ex.: access=false com edit=true) → bloquear com mensagem.
2. Falha API → erro.

• **Pós-condições:** Permissões persistidas e auditadas.

• **Integração:** IN08 — GET /api/seguranca/permissoes; IN09 — POST/PUT /api/seguranca/permissoes

## **Caso de Uso UC06**: Autorizar Ação (consumo FE/BE)

**Descrição:** Validar permissões em tempo de execução no front/back.

• **Ator Primário:** Sistema (submódulos consumidores)

• **Pré-condições:**

1. Usuário autenticado.
2. Grupo do usuário determinado.

• **Fluxo Principal:**

1. Front-end carrega GET /api/auth/me/permissions no login.
2. FE oculta/desabilita ações não permitidas.
3. BE aplica decorator/policy e, se permitido, executa a ação.

• **Fluxo Alternativo:**

1. Permissão negada → 403 com payload padronizado.
2. Falha API → erro e fallback UX.

• **Pós-condições:** Ação autorizada ou negada com UX coerente.

• **Integração:** POST /api/auth/authorize; GET /api/auth/me/permissions

## **Caso de Uso UC07:** Sincronizar Catálogo (Seed/Sync)

**Descrição:** Cadastrar/atualizar catálogo conforme menu/manifesto.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado com permissão de sync.
2. Manifesto/menu disponível.

• **Fluxo Principal:**

1. Acionar 'Sincronizar'.
2. Sistema lê manifesto/menu.
3. Cria/atualiza módulos/submódulos sem duplicar codes.
4. Exibe relatório (adicionados/alterados).

• **Fluxo Alternativo:**

1. Inconsistências de code → relatório de pendências.
2. Falha API → erro.

• **Pós-condições:** Catálogo atualizado e auditado.

• **Integração:** IN12 — POST /api/seguranca/catalogo/sync

## **Caso de Uso UC08:** Copiar/Importar/Exportar (opcional)

**Descrição:** Copiar permissões entre grupos e importar/exportar CSV/JSON.

• **Ator Primário:** Administrador

• **Pré-condições:**

1. Usuário autenticado.
2. Grupos e/ou arquivo válidos.

• **Fluxo Principal:**

1. Abrir modal de Copiar ou Importar/Exportar.
2. Selecionar origem/destinos ou arquivo.
3. Confirmar operação.
4. Sistema valida schema e aplica mudanças.

• **Fluxo Alternativo:**

1. Erros de validação → relatório com linhas afetadas.
2. Falha API → erro.

• **Pós-condições:** Permissões copiadas/importadas/exportadas e auditadas.

• **Integração:** IN10 — POST copiar permissões; IN11 — POST/GET importar|exportar

# 9. Interface do Usuário (referência)

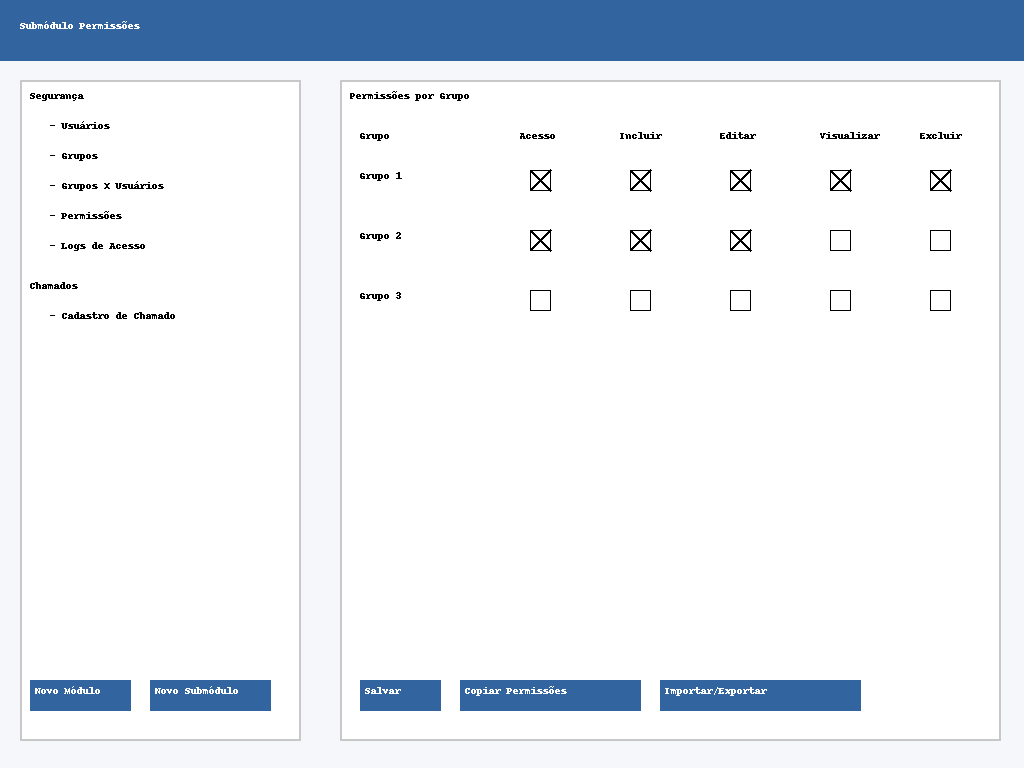
9.1 Estrutura Geral da Tela  
•Painel de Árvore (esquerda) com Módulos/Submódulos (expandir/contrair).  
• Painel da Matriz (direita) com tabela: Grupo | Acesso | Incluir | Editar | Visualizar | Excluir.  
• Barra de ações: Novo Módulo, Novo Submódulo, Salvar, Copiar Permissões, Importar/Exportar.  
• Mensagens padrão e paginação quando aplicável.

9.2 Árvore  
• Busca por nome; indicador Ativo/Inativo.  
• Ações por item: Novo Submódulo, Editar, Excluir (com confirmações e bloqueios).

9.3 Matriz de Permissões  
• Edição inline via checkboxes; validação em tempo real de pré-requisito (access).  
• Botões 'Salvar' (lote/linha) e 'Desfazer' alterações.  
• Mensagens de vazio e sucesso/erro.

9.4 Modais  
• Novo/Editar Módulo: Nome\*, module\_code\*, Descrição, Ativo.  
• Novo/Editar Submódulo: Módulo selecionado, submodule\_code\*, Nome, Rota, Ativo.  
• Excluir: confirmação com impactos.  
• Copiar Permissões: Origem, Destinos (multi), Escopo (Módulo/Submódulo).  
• Importar/Exportar: seleção de arquivo/ação e preview.

Exemplo:



# 10. Dados e Integrações

Principais rotas:  
• IN01 – GET /api/seguranca/modulos?include=submodulos  
• IN02 – POST /api/seguranca/modulos  
• IN03 – PUT/PATCH /api/seguranca/modulos/{id}  
• IN04 – DELETE /api/seguranca/modulos/{id}  
• IN05 – POST /api/seguranca/submodulos  
• IN06 – PUT/PATCH /api/seguranca/submodulos/{id}  
• IN07 – DELETE /api/seguranca/submodulos/{id}  
• IN08 – GET /api/seguranca/permissoes?moduloId=&submoduloId=  
• IN09 – POST/PUT /api/seguranca/permissoes  
• IN10 – POST /api/seguranca/permissoes/copiar  
• IN11 – POST/GET /api/seguranca/permissoes/importar|exportar  
• IN12 – POST /api/seguranca/catalogo/sync  
• /api/auth/authorize (pontual) e /api/auth/me/permissions (cache)

# 11. Mensagens do Sistema

* “Módulo/Submódulo criado/atualizado/excluído com sucesso”.
* “Permissões salvas com sucesso”.
* “Operação não permitida”. “Nenhum item encontrado”.
* “Erro de comunicação com servidor”.

# 12. Considerações de LGPD e Segurança

Acesso restrito a administradores. Auditoria nas operações de escrita. Não há tratamento de dados pessoais sensíveis neste submódulo. Anonimizar IP de logs após 180 dias.

# 13. Estrutura de Dados (Proposta)

**Tabelas (PostgreSQL):**  
• seguranca\_modulo: id BIGSERIAL PK; module\_code VARCHAR(80) UNIQUE NOT NULL; nome VARCHAR(120) NOT NULL; descricao VARCHAR(255); ativo BOOL DEFAULT TRUE; criado\_em/atualizado\_em TIMESTAMPTZ; criado\_por/atualizado\_por BIGINT.  
• seguranca\_submodulo: id BIGSERIAL PK; modulo\_id BIGINT FK(seguranca\_modulo.id) NOT NULL; submodule\_code VARCHAR(80) NOT NULL; nome VARCHAR(120) NOT NULL; rota VARCHAR(180); ativo BOOL DEFAULT TRUE; UNIQUE(modulo\_id, submodule\_code); criado\_em/atualizado\_em; criado\_por/atualizado\_por.  
• seguranca\_permissao\_grupo: id BIGSERIAL PK; grupo\_id BIGINT FK(grupos.id) NOT NULL; modulo\_id BIGINT NULL FK(seguranca\_modulo.id); submodulo\_id BIGINT NULL FK(seguranca\_submodulo.id); access BOOL DEFAULT FALSE; create BOOL DEFAULT FALSE; edit BOOL DEFAULT FALSE; view BOOL DEFAULT FALSE; delete BOOL DEFAULT FALSE; CONSTRAINT chk\_alvo CHECK ((modulo\_id IS NOT NULL) OR (submodulo\_id IS NOT NULL)); UNIQUE(grupo\_id, modulo\_id, submodulo\_id).  
• seguranca\_auditoria: id BIGSERIAL PK; entidade VARCHAR(60); entidade\_id BIGINT; acao VARCHAR(30); antes JSONB; depois JSONB; executado\_por BIGINT; executado\_em TIMESTAMPTZ DEFAULT NOW().

**Relacionamentos e Observações:**  
• (seguranca\_modulo 1—N seguranca\_submodulo)  
• (grupos 1—N seguranca\_permissao\_grupo) com alvo: módulo OU submódulo  
• Precedência: permissões no submódulo prevalecem sobre módulo (regra de negócio RN-A4)  
• Imutabilidade de codes (RN-A1); nomes podem mudar sem quebrar regras

**Índices sugeridos:**  
• IX\_modulo\_code ON seguranca\_modulo(module\_code)  
• IX\_submodulo\_code ON seguranca\_submodulo(modulo\_id, submodule\_code)  
• IX\_perm\_grupo\_alvo ON seguranca\_permissao\_grupo(grupo\_id, modulo\_id, submodulo\_id)  
• IX\_perm\_lookup ON seguranca\_permissao\_grupo(modulo\_id, submodulo\_id)

**View sugerida:**  
• vw\_permissoes\_efetivas(grupo\_id, modulo\_id, submodulo\_id, access, create, edit, view, delete)  
 — Calcula a permissão efetiva aplicando precedência (submódulo > módulo).  
  
**Auditoria:**  
• Triggers em INSERT/UPDATE/DELETE de seguranca\_modulo, seguranca\_submodulo, seguranca\_permissao\_grupo para gravar antes/depois em seguranca\_auditoria.

# 14. Referências do Projeto

*Os arquivos abaixo são os guias oficiais deste projeto e servem como referência normativa para front‑end, back‑end, integração e nomenclatura. A implementação deve observar estritamente estes materiais.*

|  |  |
| --- | --- |
| **Arquivo** | **Descrição** |
| A-react\_guide.md | Guia de front‑end (padrões de componentes, UX, grid, modal, tooltip, truncamento visual, acessibilidade). |
| A-guia\_fastapi.md | Guia de back‑end (FastAPI): estrutura de rotas, validação, handlers de erro, observabilidade. |
| NomenclatureGuide.md | Padrões de nomenclatura: DDD, nomes de módulos, rotas, DTOs e eventos. |
| A-integration\_guide.md | Integrações externas e internas: contratos, autenticação, timeouts, políticas de retry e mensagens de erro. |

# 15. Mapa de Integrações

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Título** | **Escopo** | **Documento** |
| **IN01** | **Listar Estrutura** | **GET /api/seguranca/modulos?include=submodulos** | **A-integration\_guide.md (§IN01)** |
| **IN02** | **Cadastrar Módulo** | **POST /api/seguranca/modulos** | **A-integration\_guide.md (§IN02)** |
| **IN03** | **Editar Módulo** | **PUT/PATCH /api/seguranca/modulos/{id}** | **A-integration\_guide.md (§IN03)** |
| **IN04** | **Excluir Módulo** | **DELETE /api/seguranca/modulos/{id}** | **A-integration\_guide.md (§IN04)** |
| **IN05** | **Cadastrar Submódulo** | **POST /api/seguranca/submodulos** | **A-integration\_guide.md (§IN05)** |
| **IN06** | **Editar Submódulo** | **PUT/PATCH /api/seguranca/submodulos/{id}** | **A-integration\_guide.md (§IN06)** |
| **IN07** | **Excluir Submódulo** | **DELETE /api/seguranca/submodulos/{id}** | **A-integration\_guide.md (§IN07)** |
| **IN08** | **Exibir Permissões** | **GET /api/seguranca/permissoes?moduloId=&submoduloId=** | **A-integration\_guide.md (§IN08)** |
| **IN09** | **Salvar Permissões** | **POST/PUT /api/seguranca/permissoes** | **A-integration\_guide.md (§IN09)** |
| **IN10** | **Copiar Permissões** | **POST /api/seguranca/permissoes/copiar** | **A-integration\_guide.md (§IN10)** |
| **IN11** | **Importar/Exportar** | **POST/GET /api/seguranca/permissoes/importar|exportar** | **A-integration\_guide.md (§IN11)** |
| **IN12** | **Sincronizar Catálogo** | **POST /api/seguranca/catalogo/sync** | **A-integration\_guide.md (§IN12)** |

# 16. Integração com o Projeto Existente (Resumo)

⚠️ IMPACTO OBRIGATÓRIO NO CÓDIGO DOS DEMAIS SUBMÓDULOS.

Os submódulos já existentes (Usuários, Grupos, Grupos X Usuários, Logs de Acesso, Chamados) DEVEM ser alterados para consumir e aplicar as permissões definidas por este submódulo.  
• Front-end: inclusão de guards para bloquear/ocultar telas e ações (Acesso, Incluir, Editar, Visualizar, Excluir) conforme as permissões carregadas via GET /api/auth/me/permissions.  
• Back-end: inclusão de policies/decorators em cada endpoint; negar com HTTP 403