Módulo de Autenticação (Login/Sessão)

Base Path: /auth
Finalidade: Gerenciar o processo de login e o ciclo de vida do token de sessão.

1. Login (Obter Token de Sessão)

Este é o endpoint principal para a autenticação do usuário.
Atores: Todos (Administrador, Professor, Aluno)

Parâmetro	Método	Rota	Descrição
Request Body	POST	/auth/login	Realiza o login e retorna o token de autenticação (ex: Firebase ID Token).

Corpo da Requisição (JSON Exemplo):

```
{
  "email": "usuario@exemplo.com",
  "password": "senha_minimo_8_caracteres"
}
```

Regras de Negócio Críticas ([RNF03]):

1. **Sucesso no Login:** O endpoint deve se comunicar com o Firebase Auth para validar as credenciais.
2. **Retorno:** O endpoint deve retornar o **Firebase ID Token**.
3. **Mecanismo de Sessão:** O cliente deve usar este token para manter a sessão (idealmente em um cookie httpOnly com expiração de **30 minutos** ou via cabeçalho Authorization para Single Page Applications).

2. Validação do Token (Interno)

A validação do token é feita via middleware em outras rotas (ex: GET /alunos) e não é um endpoint de API público:

- **Mecanismo:** O middleware utiliza o AuthService.verifyToken(idToken) (que chama admin.auth().verifyIdToken()) para decodificar o token e obter o uid e o tipo do usuário, garantindo a permissão.
- **Falha:** Falha na validação deve resultar em erro 401 Unauthorized.

3. Logout (Encerrar Sessão)

Embora não especificado no DRE, é uma rota essencial para a segurança.
Atores: Usuários logados

Parâmetro	Método	Rota	Descrição
Headers	POST	/auth/logout	Invalida o token de sessão (seja no lado do cliente ou do servidor).

Regra de Negócio:

1. Se a aplicação usa tokens JWT/Firebase ID Token (stateless), o logout deve instruir o cliente a descartar o token e/ou invalidar a sessão no lado do servidor (se for um *refresh token* ou sessão de cookie).