Plano de Testes – ServeRest API

1. Apresentação

Este plano revisado descreve a estratégia de testes da API ServeRest, consolidando o planejamento inicial e as melhorias encontradas durante a execução do Challenge.

O documento foi ajustado após feedback dos instrutores, incorporando:

- Análise crítica das mensagens de erro.
- Detalhamento das evidências.
- Alinhamento entre o planejamento inicial e os testes efetivamente executados.

2. Pessoas Envolvidas

- **Responsável:** Emanuel Felipe Avelino Silva

3. Objetivo

Garantir que as regras de negócio da API sejam cumpridas, validando fluxos principais, alternativos e cenários de erro, com foco em qualidade, clareza das mensagens retornadas e robustez.

4. Escopo

4.1 Dentro do escopo

- Rotas: /usuarios, /login, /produtos, /carrinhos.
- Operações: POST, GET, PUT, DELETE (CRUD completo quando aplicável).
- Regras de negócio:
    - Unicidade de e-mails.
    - Restrição de provedores (gmail/hotmail).
    - Validação de senhas (mínimo 5, máximo 10 caracteres).
    - Apenas usuários autenticados e administradores podem gerenciar produtos.
    - Um usuário pode ter apenas um carrinho ativo.

4.2 Fora do escopo

- Integrações externas.
- Testes de carga, stress e performance.
- Testes de segurança avançados.

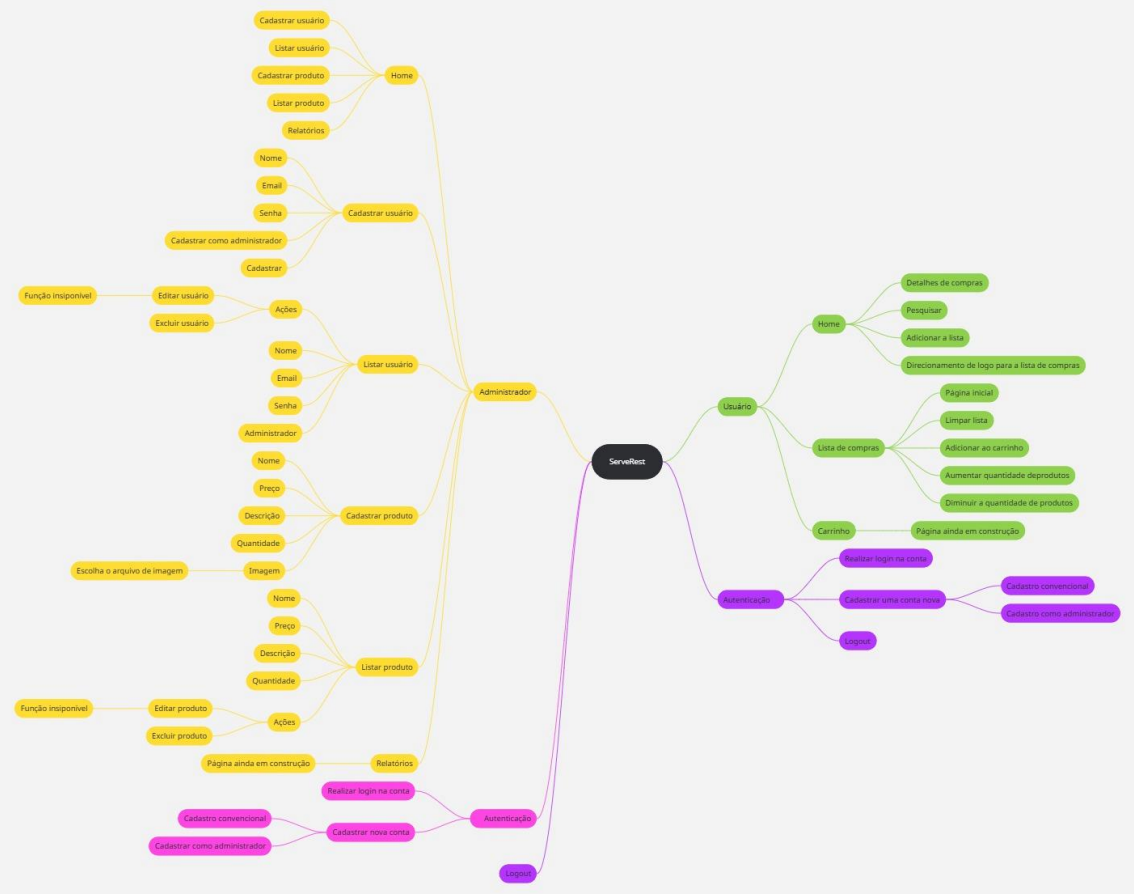
5. Estratégia de Testes

1. **Execução manual exploratória** com Postman para validar regras de negócio.
2. **Execução estruturada** com QAlity (Jira), registrando cenários planejados, resultados e bugs.
3. **Automação com Robot Framework** nos cenários críticos, para acelerar execuções repetitivas.
4. **Feedback contínuo**: evolução do plano com base nos resultados.

6. Técnicas Aplicadas

- Testes funcionais manuais (Postman).
- Testes exploratórios.
- Testes de limite (senhas, e-mails, mensagens de erro).
- Automação de API (Robot Framework + RequestsLibrary).

7. Mapa mental



8. Diferenças entre o Plano Inicial e a Execução Real

- O **plano inicial** previa 11 cenários básicos, cobrindo apenas fluxos positivos/negativos de usuários, login e produtos.
- A **execução real** expandiu para **42 cenários** (15 usuários, 4 login, 12 produtos, 11 carrinhos), cobrindo também:
    - Casos de **limite** (senhas curtas/longas, e-mails proibidos).
    - **Mensagens de erro pouco claras** (cadastro duplicado, exclusão de inexistentes, carrinho concluído/cancelado em duplicidade).
    - Cenários exploratórios não previstos (atualização criando registros automaticamente).

9. Cenários de Teste Planejados (Revisado)

Usuários

- Cadastrar usuário válido (201).
- Cadastrar usuário duplicado (400).
- Cadastrar usuário com senha < 5 caracteres.
- Cadastrar usuário com senha > 10 caracteres.
- Cadastrar usuário com e-mail de provedores proibidos.
- Cadastrar usuário com e-mail inválido (400).
- Atualizar usuário inexistente → deve retornar erro.
- Deletar usuário inexistente → mensagem clara esperada.
- Deletar usuário já excluído → mensagem clara esperada.

Login

- Login com credenciais válidas → 200 + token.
- Login com senha inválida → 401.
- Login com usuário inexistente → 401.
- Login sem body → 400.
- Login com e-mail inválido → 400.

Produtos

- Cadastro de produto válido (201).
- Cadastro de produto duplicado (400 – mensagem deve ser clara).
- Cadastro sem autenticação → 401.
- Atualizar produto válido (200).

- Atualizar produto com ID inexistente.
- Excluir produto válido (200).
- Excluir produto inexistente.
- Acesso com usuário não-admin → 403.

Carrinhos

- Criar carrinho válido (201).
- Criar carrinho duplicado → 400.
- Buscar carrinho inexistente → 400.
- Concluir compra (200).
- Concluir compra duplicada.
- Cancelar compra (200).
- Cancelar compra duplicada.
- Cancelar compra com token inválido → 401.

10. Priorização

- **Alta prioridade:** Login, cadastro de usuários, cadastro de produtos.
- **Média prioridade:** Atualizações e exclusões.
- **Baixa prioridade:** Consultas de registros inexistentes.

11. Matriz de Risco

- **Crítico:** Falhas em login e cadastro (usuário/produto).
- **Alto:** Mensagens de erro genéricas → impactam a usabilidade.
- **Moderado:** Problemas em carrinhos.
- **Baixo:** Consultas a registros inexistentes.

12. Candidatos à Automação

12.1 Critérios de Seleção

Os cenários foram selecionados para automação com base nos seguintes critérios:

1. **Criticidade**: Cenários que validam funcionalidades essenciais para o negócio
2. **Repetitividade**: Testes que precisam ser executados frequentemente (regressão)
3. **Estabilidade**: Cenários com comportamento previsível e interface estável (API REST)
4. **ROI (Retorno sobre Investimento)**: Relação custo-benefício da automação vs execução manual

5. **Complexidade de dados**: Cenários que requerem múltiplas combinações de dados

12.2 Cenários Selecionados para Automação

Módulo: Login

ID	Cenário	Status Code	Criticidade	Motivo da Automação
CT-L01	Login válido	200 + token	Alta	Pré-requisito para todas operações autenticadas
CT-L03	Login com senha inválida	401	Alta	Validação de segurança crítica

Não automatizados: Login sem body, Login com email inválido Motivo: Baixa complexidade, validação simples de campos obrigatórios

Motivo: Baixa complexidade, validação simples de campos obrigatórios, execução manual rápida.

Módulo: Usuários

ID	Cenário	Status Code	Criticidade	Motivo da Automação
US-03	Cadastrar usuário válido	201	Alta	Fluxo principal da aplicação
US-07	Cadastrar usuário duplicado	400	Alta	Validação de regra de negócio crítica
US-05	Senha < 5 caracteres	201 (bug)	Alta	Valida bug crítico identificado
US-06	Senha > 10 caracteres	201 (bug)	Alta	Valida bug crítico identificado
US-04	Email Gmail/Hotmail	201 (bug)	Alta	Valida bug crítico identificado

Não automatizados: Buscas, atualizações e exclusões Motivo: Validações de mensagens requerem análise crítica humana, ROI baixo

Motivo:

- Operações de consulta/atualização têm menor impacto no negócio
- Testes exploratórios manuais são mais eficientes para validar mensagens de erro
- Baixa repetitividade comparado aos fluxos principais

Módulo: Produtos

ID	Cenário	Status Code	Criticidade	Motivo da Automação
PR-03	Cadastrar produto válido	201	Alta	Essencial para fluxo de carrinhos
PR-01	Cadastrar sem autenticação	401	Alta	Validação de segurança
PR-10	Excluir produto válido	200	Média	Necessário para limpeza de dados nos testes

Não automatizados: Produtos duplicados, buscas, atualizações Motivo: Cenários de validação de mensagens são melhor verificados manualmente

Motivo:

- Cenários de validação de mensagens são melhor verificados manualmente
- Testes exploratórios capturam nuances que automação pode não detectar
- ROI baixo para cenários de erro menos críticos

Módulo: Carrinhos

ID	**Cenário**	**Status Code**	**Criticidade**	**Motivo da Automação**
CA-04	Criar carrinho válido	201	Alta	Fluxo principal de negócio
CA-07	Concluir compra	200	Alta	Simula jornada completa do usuário

Não automatizados: Carrinho duplicado, cancelar compra, buscas Motivo: Cenários de exceção têm menor impacto, mensagens requerem validação manual

Motivo:

- Validações de regras de negócio específicas são mais ágeis manualmente

- Mensagens de erro requerem análise crítica humana
- Cenários de exceção têm menor impacto em produção

12.3 Cobertura de Automação

Resumo quantitativo:

Módulo	Total de Cenários	Automatizados	% Cobertura	Prioridade
Login	4	2	50%	Alta
Usuários	15	5	33%	Alta
Produtos	12	3	25%	Media
Carrinhos	11	2	18%	Alta
Total	42	12	29%	-