

Cenários de Teste (Test Scenarios)

1. Objetivo

Definir **cenários de teste de alto nível** que representam comportamentos críticos do sistema de Encurtamento de URLs.

Os cenários servem como base para derivação de **casos de teste**, automação e validação de requisitos funcionais, não funcionais e de segurança.

2. Escopo

Inclui:

- Fluxos principais do negócio
- Cenários negativos e de exceção
- Cenários de segurança derivados do Threat Model
- Cenários de desempenho e custo relevantes ao MVP

Exclui:

- Funcionalidades fora do MVP
- Cenários administrativos inexistentes

3. Cenários Funcionais

SC-F-01 — Criar URL Curta com URL Válida

Dado uma URL pública válida

Quando o cliente solicita a criação

Então o sistema retorna uma URL curta única

SC-F-02 — Redirecionar URL Curta Existente

Dado uma URL curta válida

Quando ela é acessada

Então o sistema redireciona para a URL original com HTTP 301 ou 302

SC-F-03 — Criar URLs Distintas para Entradas Diferentes

Dado múltiplas URLs válidas

Quando são criadas

Então cada uma recebe um identificador único

SC-F-04 — Acessar URL Expirada

Dado uma URL curta expirada

Quando é acessada

Então o sistema retorna resposta apropriada (não encontrada ou equivalente)

4. Cenários de Validação

SC-V-01 — Rejeitar URL Malformada

Dado uma URL inválida

Quando a criação é solicitada

Então o sistema rejeita a requisição

SC-V-02 — Rejeitar Domínio ou TLD Bloqueado

Dado uma URL com domínio proibido

Quando a criação é solicitada

Então o sistema rejeita a requisição

5. Cenários de Segurança

SC-S-01 — Bloquear SSRF por IP Privado

Dado uma URL apontando para IP privado

Quando a criação é solicitada

Então o sistema bloqueia a requisição

SC-S-02 — Bloquear Loopback

Dado uma URL apontando para 127.0.0.1

Quando a criação é solicitada

Então o sistema bloqueia a requisição

SC-S-03 — Bloquear Metadata Cloud

Dado uma URL apontando para serviço de metadata

Quando a criação é solicitada

Então o sistema bloqueia a requisição

SC-S-04 — Mitigar Enumeração de Identificadores

Dado múltiplas tentativas sequenciais de acesso

Quando o padrão indica enumeração

Então o sistema aplica mitigação (rate limiting ou degradação)

SC-S-05 — Mitigar DoS / EDoS

Dado alto volume de requisições automatizadas

Quando o limite é atingido

Então o sistema aplica rate limiting sem indisponibilidade total

6. Cenários Não Funcionais

SC-NF-01 — Latência de Redirecionamento

Dado uma URL curta válida

Quando é acessada

Então o redirecionamento ocorre dentro do limite definido no SRS

SC-NF-02 — Observabilidade

Dado uma requisição válida ou inválida

Quando é processada

Então logs e métricas são gerados sem dados sensíveis