Modelo de Ameaças (Threat Model)

1. Objetivo

Este documento identifica, analisa e classifica as ameaças de segurança associadas ao sistema de Encurtamento de URLs, com base nos requisitos definidos na Especificação de Requisitos do Sistema (SRS).

O objetivo é:

- Compreender como o sistema pode ser atacado
- Avaliar riscos técnicos e de negócio
- Definir controles de mitigação antes da implementação

Este modelo de ameaças orienta decisões de arquitetura, validações, controles de segurança e testes.

---

2. Escopo do Modelo de Ameaças

O escopo inclui os seguintes componentes:

- Endpoint de criação de URLs curtas
- Endpoint de redirecionamento
- API Gateway
- Funções AWS Lambda
- Banco de dados DynamoDB
- Logs e métricas (CloudWatch)

Componentes fora do escopo:

- Autenticação de usuários
- Painéis administrativos
- Integrações externas não previstas no MVP

3. Ativos a Proteger

Os principais ativos do sistema são:

- Integridade do redirecionamento (URL curta → URL original correta)
- Reputação do domínio do serviço
- Disponibilidade do sistema
- Infraestrutura interna da cloud
- Custos operacionais
- Dados de configuração e políticas

4. Superfície de Ataque

As principais superfícies de ataque identificadas são:

- Entrada de URLs fornecidas por clientes
- Parâmetros do endpoint de redirecionamento
- Geração e resolução de identificadores curtos
- Persistência e leitura no banco NoSQL
- Logs e mensagens de erro

5. Ameaças Identificadas (Classificação STRIDE)

5.1 Spoofing (Falsificação)

Ameaça:
Uso do serviço para mascarar destinos maliciosos, induzindo usuários a confiar no domínio do encurtador.

Impacto:
Danos à reputação, bloqueio do domínio por navegadores e provedores.

Mitigação:

- Validação rigorosa de URLs
- Bloqueio de domínios e TLDs proibidos
- Políticas explícitas de aceitação de URLs

5.2 Tampering (Manipulação)

Ameaça:
Tentativa de alterar mapeamentos de URLs ou explorar falhas na geração de identificadores.

Impacto:
Redirecionamentos incorretos ou maliciosos.

Mitigação:

- Identificadores imutáveis
- Ausência de endpoints de alteração no MVP
- Persistência controlada via chave primária única

5.3 Repudiation (Repúdio)

Ameaça:
Impossibilidade de auditar ações maliciosas ou abusivas.

Impacto:
Dificuldade de investigação e resposta a incidentes.

Mitigação:

- Logs estruturados
- Registro de eventos de criação e acesso
- Correlação mínima por requisição

5.4 Information Disclosure (Divulgação de Informação)

Ameaça:
Exposição de dados sensíveis por meio de respostas ou logs.

Impacto:
Vazamento de informações internas ou de usuários.

Mitigação:

- Logs sem dados sensíveis
- Mensagens de erro genéricas
- Não exposição desnecessária de URLs completas

5.5 Denial of Service (DoS) e Economic Denial of Service (EDoS)

Ameaça:
Envio massivo e automatizado de requisições aos endpoints de criação ou redirecionamento com o objetivo de:

- Degradar a disponibilidade do serviço
- Provocar aumento significativo de custos em ambiente serverless

Impacto:

- Elevação abrupta de custos operacionais (Lambda, API Gateway, DynamoDB)
- Possível throttling do serviço
- Indisponibilidade para usuários legítimos

Mitigação:

- Rate limiting no API Gateway
- Limitação de requisições por IP ou padrão de uso
- TTL obrigatório para registros persistidos
- Monitoramento de métricas de volume e custo
- Alarmes de custo e uso anômalo

Classificação STRIDE:

- Denial of Service

5.6 Elevation of Privilege (Elevação de Privilégio)

Ameaça:
Exploração do serviço para acessar recursos internos da infraestrutura por meio de SSRF.

Impacto:
Comprometimento de credenciais, dados ou serviços internos.

Mitigação:

- Bloqueio de IPs privados e loopback
- Bloqueio de serviços de metadata cloud
- Resolução e validação de DNS antes da persistência

6. Riscos Residuais

Mesmo com as mitigações definidas, os seguintes riscos são considerados residuais e aceitáveis no contexto do MVP:

- Uso pontual do serviço para redirecionamento de conteúdo indesejado, mitigado por monitoramento
- Tentativas de abuso de baixo volume, mitigadas por rate limiting

Esses riscos devem ser monitorados continuamente.

7. Controles de Segurança Derivados

Este modelo de ameaças gera os seguintes controles obrigatórios:

- Validação defensiva de URLs
- Políticas explícitas de aceitação e bloqueio
- Rate limiting
- TTL obrigatório
- Monitoramento de custo
- Logs estruturados e observáveis

Esses controles devem ser refletidos na arquitetura, no código e na infraestrutura.

8. Conclusão

O encurtador de URLs é um serviço sensível cujo principal risco não é apenas técnico, mas **reputacional, operacional e financeiro**.
Este modelo de ameaças estabelece as bases para uma arquitetura defensiva, orientada a risco, desde a concepção do sistema