Modelagem de Ameaças - Gestão de TCCs

Proprietário: David Almeida
Revisor: David Almeida
Contribuidores: David Almeida, Edson Valença, José Gabriel, Mariana Cavalcanti
Data Gerada: Mon Apr 14 2025

OWASP Threat Dragon

Resumo Executivo

Descrição de alto nível do sistema (high level system)

O Projeto de Gestão de TCC tem como objetivo tornar a supervisão e o acompanhamento dos TCCs mais eficientes, minimizando problemas enfrentados pelos orientadores e garantindo maior organização no fluxo de trabalho. A plataforma permitirá a digitalização e assinatura eletrônica de documentos, reduzindo burocracias e agilizando processos.

Resumo

Ameaças totais	23
Total Mitigado	0
Não atenuado	23
Abrir / Alta Prioridade	0
Abrir / Prioridade Média	0
Abrir / Baixa Prioridade	0
Prioridade Aberta / Desconhecida	0

Diagrama STRIDE - Gestão de TCCs

Diagrama de modelagem de ameaças usando o Threat Dragon e a metodologia STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).

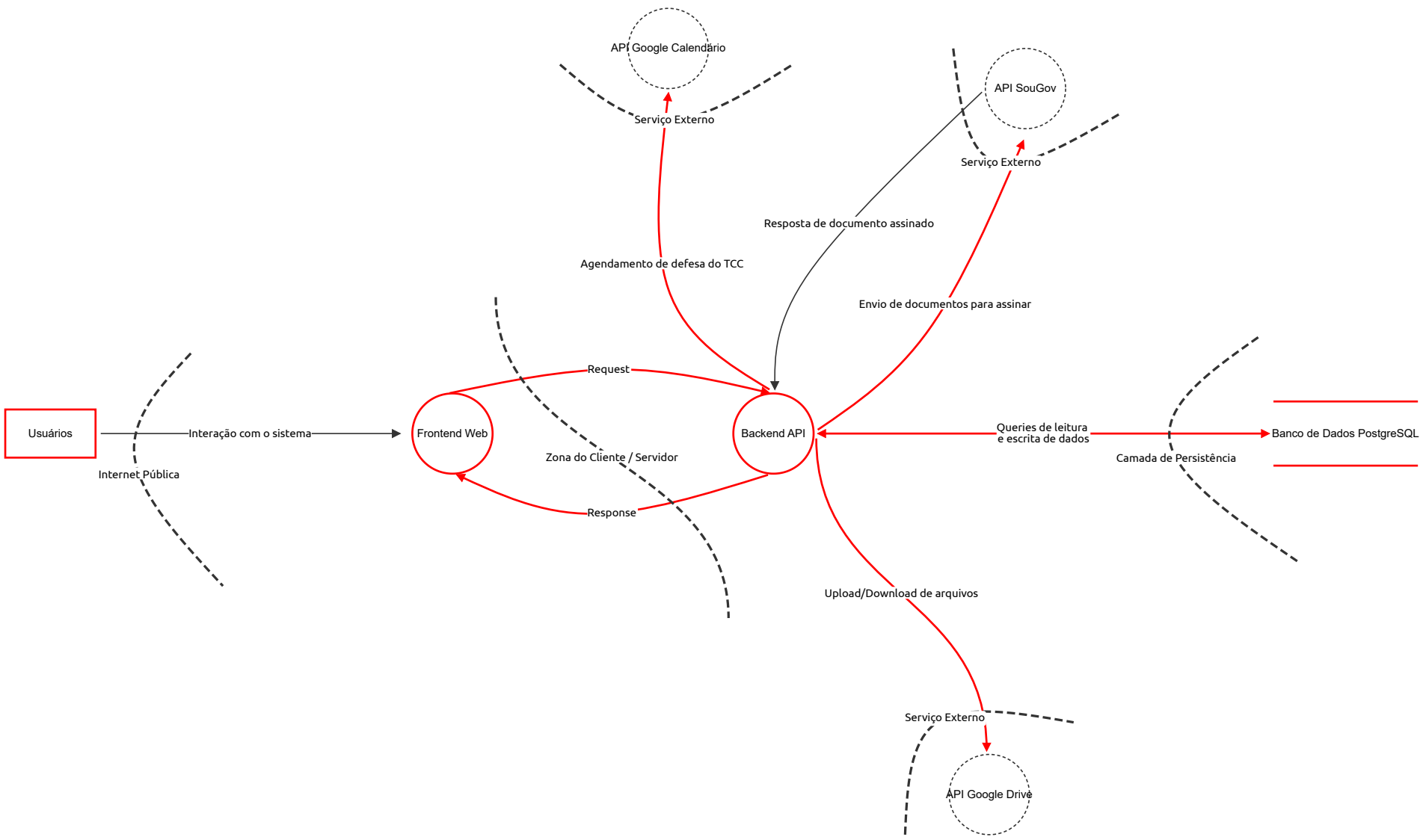

Diagrama STRIDE - Gestão de TCCs

Usuários (Ator)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Negação de ações realizadas	Repudiation	TBD	Open		Um usuário alega não ter assinado um documento, mesmo tendo feito isso.	Registro de logs imutáveis com IP, timestamp e id do usuário, notificações por e-mail confirmando ações importantes.
2	Acesso de usuário não autorizado	Spoofing	TBD	Open		Um invasor tenta se passar por um usuário legítimo usando e-mail e senha roubados.	Tokens de primeiro acesso com validade curta, bloqueio após tentativas incorretas

Frontend Web (Processo)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Uso de sessão roubada	Spoofing	TBD	Open		Invasor acessa o sistema com um token de sessão roubado.	Tokens curtos com expiração.
10	Manipulação do JavaScript	Tampering	TBD	Open		Alguém injeta código malicioso no frontend.	Content Security Policy (CSP)
11	Alterar dados do DOM para acessar funções	Elevation of privilege	TBD	Open		Alguém altera atributos do HTML para ativar recursos de admin.	Autorização sempre feita no backend, nunca confiar no DOM.

Backend API (Processo)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Acesso à API com token inválido ou forjado	Spoofing	TBD	Open		Alguém forja um JWT ou token de autenticação.	Assinatura forte dos tokens, validação com expiração.
13	Manipulação de parâmetros na API	Tampering	TBD	Open		Modificação de parâmetros para acessar dados de outro usuário.	Controle de acesso baseado em contexto no backend.
14	Falta de rastreabilidade das requisições	Repudiation	TBD	Open		Ações não são associadas de forma auditável ao usuário que as fez.	Logging detalhado com ID do usuário, IP e ação.

Banco de Dados PostgreSQL (Armazenamento)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Usuário nega que alterou dados	Repudiation	TBD	Open		Alguém diz que não modificou o status de um TCC.	Logging com quem fez a alteração, e quando.
21	Vazamento por má configuração	Information disclosure	TBD	Open		Banco de dados exposto na internet ou má configuração de roles.	Acesso apenas por rede privada, roles com mínimo privilégio.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
22	Consulta pesada sem índice ou com injeção	Denial of service	TBD	Open		Ataques com queries pesadas que travam o banco.	Limitação de tempo de execução, monitoração e otimização de queries.
24	Senhas visíveis no banco	Information disclosure	TBD	Open		Não utilização de criptografia para as senhas dos usuários	Hashing com salt nas senhas

API SouGov (Processo) *- Fora do Escopo*

Razão por estar fora de escopo: É uma API externa

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

API Google Drive (Processo) *- Fora do Escopo*

Razão por estar fora de escopo: É uma API externa

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Modificação de requisição	Tampering	TBD	Open		Alguém intercepta e altera uma requisição do frontend ao backend.	Uso de HTTPS com TLS, validação de dados no backend.
6	Ataque DDoS via requisições maliciosas	Denial of service	TBD	Open		O backend é sobrecarregado por múltiplas requisições maliciosas.	Validação e sanitização de entrada, limitação de taxa (rate limiting)
23	Vazamento de informações	Information disclosure	TBD	Open		Informações pessoais nos parâmetros da URL	HTTPS, não usar GET para dados sensíveis

Response (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Vazamento de dados na resposta	Tampering	TBD	Open		A resposta do backend inclui dados sensíveis além do necessário.	Minimização de dados em resposta, mascaramento de informações sensíveis.
8	Manipulação de resposta do backend	Tampering	TBD	Open		Um agente intercepta e modifica a resposta antes que ela chegue ao frontend.	HTTPS end-to-end, validação de integridade no frontend.

Upload/Download de arquivos (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	Alteração maliciosa em arquivos no Google Drive	Tampering	TBD	Open		Arquivos do TCC são adulterados por usuários não autorizados.	Controle de permissões no Drive, versionamento de documentos.
16	Upload massivo ou acesso abusivo ao Drive	Denial of service	TBD	Open		Tentativa de sobrecarregar a integração com arquivos grandes.	Limites de tamanho, quotas de upload.

Envio de documentos para assinar (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	Alteração do payload antes da assinatura	Tampering	TBD	Open		Documento assinado não corresponde ao que foi enviado.	Verificação pós-assinatura.
18	Chamada excessiva à API de assinatura	Denial of service	TBD	Open		Tentativa de bloquear fluxo de assinatura com requisições sucessivas.	Limitação de requisições.

Resposta de documento assinado (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Agendamento de defesa do TCC (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
25	Alteração de detalhes de evento	Tampering	TBD	Open		Alteração das informações de data ou link da reunião online	Notificar usuários responsáveis sobre mudanças em eventos.

Queries de leitura e escrita de dados (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
19	Injeção ou modificação direta no banco	Tampering	TBD	Open		Injeção SQL altera dados de TCC.	Validação de entrada.

Interação com o sistema (Fluxo de Dados)

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

API Google Calendário (Processo) *- Fora do Escopo*

Razão por estar fora de escopo: É uma API externa

Descrição:

Number	Title	Type	Priority	Status	Score	Description	Mitigations