Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia Informática

Ano letivo 2024/2025

Tecnologias de Segurança

Trabalho Prático #1

Grupo 02

João Rodrigues - pg57880
Rúben Silva - pg57900
Miguel Guimarães - pg55986

Março 2025

Índice

1 Introdução

Neste projeto é requerido que seja desenvolvida uma **analise de segurança** do serviço *Cofre Digital*, que é um sistema que permite **guardar ficheiros** de qualquer tipo de forma segura, semelhante a plataformas como o *OneDrive* ou *Dropbox*.

O sistema encontra-se dividido em 3 componentes: **um Servidor**, **um Serviço Web** e **uma Aplicação Móvel**.

1.1 Servidor

O **servidor** contém toda a lógica do serviço que será implementado, e irá recorrer a microsserviços que se encontram em execução num ***'Cloud Provider'***. Algumas das tecnologias já utilizadas pela empresa no servidor são o *'Fedora Server 41'*, *'Nginx 1.24.0'* e *'PostgreSQL 10.22'*.

1.2 Serviço web

O ***serviço web*** atua como interface entre os utilizadores e o servidor, permitindo-lhes executar todas as ações na plataforma.

1.3 Aplicação móvel

A aplicação móvel deverá funcionar nos sistemas ***IOS*** e ***Android***, permitindo realizar todas as ações disponíveis aos utilizadores da plataforma.

A aplicação móvel mantém uma cópia dos dados do cofre para acesso *offline*. No modo *offline* é possível enviar um ficheiro do cofre para outro utilizador recorrendo a tecnologia ***bluetooth***.

A aplicação deverá ser produzida como uma ***Progressive web app***, ou seja, deverá ser desenvolvida de forma que, a partir de uma única base de código, seja possível desenvolver código tanto para a aplicação *IOS* como *Android*.

1.4 Partilha de ficheiros na plataforma

A seguir encontram-se enumeradas as ações relacionadas com a partilha de ficheiros.

- **Enviar ficheiros** para um utilizador ou um grupo de utilizadores.
- **Partilhar** uma pasta com um utilizador ou grupo de utilizadores.
- **Criar um grupo de utilizadores** utilizando os *ids* ou *e-mails* dos utilizadores que serão adicionados, o grupo crido deverá possuir um nome
- É possível definir se os utilizadores com acesso a um ficheiro partilhado o podem **repartilhar**.

1.5 Objetivos de segurança

É preciso garantir a **confidencialidade do cofre** e das **comunicações**. Para o cofre ser confidencial, é necessário garantir que o cofre apenas se encontra acessível por entidades autorizadas. A confidencialidade nas comunicações terá de ser garantida, impedindo que a comunicação seja interpretada por uma entidade não desejada.

É preciso garantir a **integridade do cofre**. Logo podemos assumir que esta integridade dos dados terá de ser cumprida tanto online (servidor) como offline (dispositivo móvel).

É preciso garantir a **autenticidade dos utilizadores**. Ou seja deve ser impedido que um utilizador falsifique a sua identidade fazendo se passar por um outro utilizador.

2 Ativos relevantes

Nesta secção serão enumerados os diversos ativos do sistema relevantes ao correto funcionamento do mesmo. Decidimos separar os dados visto serem de vital importância no sistema.

2.1 Servidor

- Servidor backend: Conjunto de microsserviços responsáveis pela lógica de negócio
- Sistema operativo (Fedora Server): Base para execução dos serviços
- Servidor web (Nginx): Gestão de conexões e balanceamento de carga
- Base de dados (PostgreSQL): Sistema de armazenamento de dados estruturados
- Middleware de autorização: Componentes que controlam permissões
- Sistema de monitorização e auditoria: Software para registo e análise de eventos do sistema
- Infraestrutura de rede cloud: Conectividade entre componentes nos servidores cloud
- Canais API: Interfaces de comunicação entre os diversos componentes do sistema
- Conexões para sistemas de backup: Canais para transferência de cópias de segurança
- DNS e serviços de resolução de nomes: Infraestrutura para localização de recursos

2.2 Serviço Web

- Serviço web: Interface web para acesso ao sistema
- Bibliotecas de criptografia: Componentes para cifrar/decifrar dados (utilizados pelo serviço web)
- Comunicações Internet: Ligações entre clientes web e o servidor
- Protocolos de comunicação segura (HTTPS, TLS): Mecanismos standards para comunicações seguras
- Redes de distribuição de conteúdos (CDN): Infraestrutura para entrega otimizada de recursos estáticos

2.3 Aplicação Móvel

- Aplicação móvel (PWA): Aplicação para dispositivos iOS e Android
- Cópias locais do cofre: Versões offline dos dados armazenados em dispositivos móveis
- Software de comunicação bluetooth: Componente que permite transferência direta entre dispositivos
- Bibliotecas de criptografia: Componentes para cifrar/decifrar dados (para operações offline e transferências Bluetooth)
- Canais de comunicação bluetooth: Ligações diretas entre dispositivos móveis para transferência P2P
- Comunicações Internet: Ligações entre clientes móveis e o servidor

2.4 Dados

- Ficheiros armazenados: Documentos, imagens, vídeos e qualquer tipo de arquivo armazenado pelos utilizadores
- Metadados dos ficheiros: Informações sobre os arquivos (tamanho, data de criação, tipo)
- Estrutura de pastas: Organização hierárquica dos ficheiros
- Credenciais de utilizadores: Nomes de utilizador, senhas, tokens de autenticação
- Dados de perfil dos utilizadores: Informações pessoais, e-mails, histórico de atividades
- Informações de grupos: Membros, permissões, identificadores
- Registos de auditoria (logs): Histórico de acesso, modificações e partilhas
- Configurações de permissões: Definições de quem pode aceder ou partilhar cada ficheiro/pasta
- Chaves criptográficas: Chaves públicas, privadas e simétricas utilizadas para proteção dos dados
- Certificados digitais: Documentos eletrônicos que atestam a identidade digital
- Cópias de segurança: Dados duplicados para recuperação em caso de falha

3 Modelação do sistema

Diagrama de Fluxo de Dados - Cofre Digital (Notação Yourdon/DeMarco)

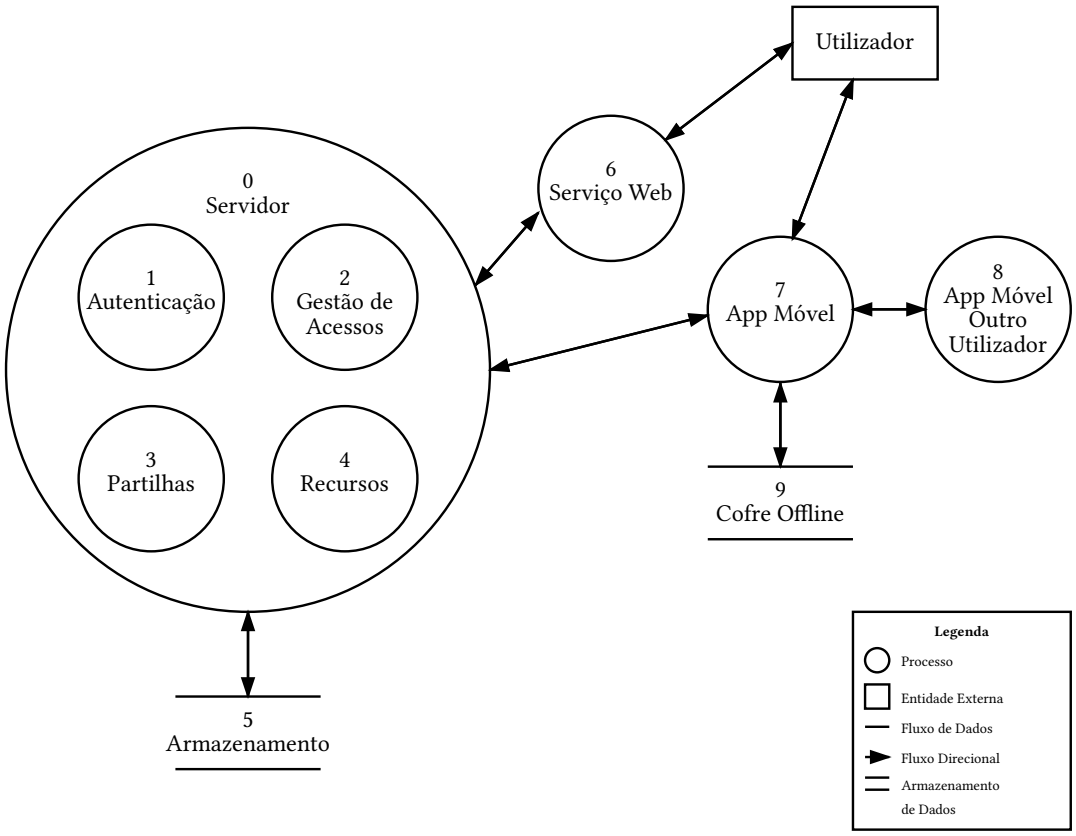

Figura 2: Fluxo de Dados (Notação de Yourdon/Demarco)

4 Principais Ameaças (STRIDE) ao Cofre Digital

A segurança do Cofre Digital é essencial para proteger os ficheiros dos utilizadores. Utilizando a metodologia STRIDE, foi identificado as principais ameaças ao sistema. Esta análise permitirá avaliar os riscos e definir medidas de segurança para garantir a confidencialidade, integridade e disponibilidade do serviço.

4.1 Servidor

4.1.1 Spoofing (Falsificação de Identidade)

- Interceção de tokens de autenticação: Captura de tokens OAuth ou JWT durante a autenticação entre a aplicação móvel/web e os microsserviços
- Falsificação de convites de grupo: Envio de convites maliciosos que parecem vir de utilizadores legítimos para obter acesso a grupos
- IP spoofing em comunicações com microsserviços: Falsificação de endereços IP entre componentes da arquitetura cloud
- API endpoint spoofing: Falsificação de endpoints de API para interceptar comunicações entre aplicação móvel e servidor

4.1.2 Tampering (Adulteração)

- Injeção de código em microsserviços: Introdução de código malicioso em microsserviços para modificar a lógica de autorização
- SQL injection: Modificação não autorizada dos dados na base de dados através de falhas na sanitização de inputs
- Comprometimento do middleware de autorização: Alteração da lógica de verificação de permissões para possibilitar acessos não autorizados
- Manipulação de payloads JSON: Alteração dos dados estruturados enviados entre componentes do sistema

4.1.3 Repudiation (Repúdio)

- Desativação seletiva de logs nos microsserviços: Manipulação dos mecanismos de registo para eliminar evidências de ações maliciosas
- Adulteração do sistema de monitorização: Modificação dos registos de auditoria para ocultar atividades suspeitas
- Manipulação de logs do PostgreSQL e Nginx: Alteração dos registos do PostgreSQL e Nginx para ocultar evidências de ataques e modificações, dificultando a sua deteção
- Mask de tráfego entre microsserviços: Ocultação de comunicações maliciosas entre componentes da arquitetura

4.1.4 Information Disclosure (Divulgação de Informação)

- Exposição de dados via falhas nos microsserviços: Leak de informações sensíveis devido a erros na implementação de APIs
- Exploração de vulnerabilidades no PostgreSQL: Obtenção de dados através da exploração de falhas na configuração da base de dados
- Sniffing em endpoints de API não protegidos: Captura e análise de tráfego em pontos vulneráveis da API
- Leak através de cabeçalhos HTTP: Exposição de informações sensíveis em cabeçalhos HTTP mal configurados

4.1.5 Denial of Service (Negação de Serviços)

- Ataques DDoS a microsserviços críticos: Sobrecarga específica de componentes essenciais da arquitetura backend
- Saturação do PostgreSQL – Execução de consultas complexas para consumir recursos da base de dados, causando exaustão das conexões disponíveis e impactando a disponibilidade do serviço.
- API rate limiting bypass: Contorno de limitações de taxa para sobrecarregar pontos de acesso específicos

4.1.6 Elevation of Privilege (Elevação de Privilégio)

- Exploração de falhas no middleware de autorização: Aproveitamento de vulnerabilidades para elevar privilégios de acesso
- Bypass da camada de autorização: Contorno dos mecanismos de verificação de permissões para acesso não autorizado
- Escalada horizontal entre microsserviços: Utilização de um microsserviço comprometido para acessar outros serviços internos
- Exploração de configurações incorretas do Nginx: Aproveitamento de falhas na configuração do servidor web para acesso não autorizado

4.2 Serviço Web

4.2.1 Spoofing (Falsificação de Identidade)

- Phishing direcionado via replicação do serviço web: Criação de páginas falsas imitando a interface do Cofre Digital para roubar credenciais
- DNS cache poisoning no acesso ao serviço web: Manipulação de resoluções DNS para redirecionar utilizadores a versões falsas do Cofre Digital

4.2.2 Tampering (Adulteração)

- Adulteração de cabeçalhos HTTP: Modificação de cabeçalhos nas requisições ao servidor para contornar validações
- Man-in-the-middle em comunicações PWA-servidor: Interseção e modificação das comunicações entre a aplicação web progressiva e os microsserviços

4.2.3 Information Disclosure (Divulgação de Informação)

- Análise de tráfego criptografado: Inferência de informações através de padrões de tráfego mesmo em comunicações cifradas
- Interseção de credenciais em conexões não-TLS: Captura de dados de autenticação em comunicações não protegidas

4.2.4 Elevation of Privilege (Elevação de Privilégio)

- Manipulação do protocolo de autenticação: Alteração do fluxo de autenticação para obter níveis de acesso superiores

4.3 Aplicação Móvel

4.3.1 Spoofing (Falsificação de Identidade)

- Bluetooth address spoofing: Falsificação de endereços Bluetooth durante transferências diretas entre dispositivos móveis

4.3.2 Tampering (Adulteração)

- Injeção de código durante sincronização offline: Modificação dos dados durante a sincronização da cópia local com o servidor
- Adulteração da PWA em cache: Modificação da Progressive Web App armazenada em cache
- Interceção de comunicações Bluetooth: Modificação de ficheiros durante transferência direta entre dispositivos em modo offline

4.3.3 Repudiation (Repúdio)

- Negação de transferência via Bluetooth: Utilizador nega ter enviado ficheiro diretamente para outro dispositivo

4.3.4 Information Disclosure (Divulgação de Informação)

- Leak de informação via cache da PWA: Extração de dados sensíveis da cache local da aplicação web progressiva

4.3.5 Denial of Service (Negação de Serviços)

- Bloqueio de sincronização: Manipulação que impede a sincronização adequada entre dispositivos e servidor
- Ataques ao sistema Bluetooth: Exploração de vulnerabilidades no software de comunicação para interromper transferências diretas

4.4 Dados

4.4.1 Spoofing (Falsificação de Identidade)

- Falsificação de propriedade na partilha de ficheiros: Utilizador falsamente aparecendo como proprietário de ficheiros partilhados
- Falsificação de metadados de autoria: Modificação dos atributos de criação para reclamar falsa autoria de documentos
- Manipulação de identificadores de grupo: Falsificação de identificadores para aparecer como membro legítimo de grupos restritos

4.4.2 Tampering (Adulteração)

- Modificação indevida de ficheiros armazenados: Alteração do conteúdo de documentos sem autorização do proprietário
- Corrupção da base de dados PostgreSQL: Manipulação dos registos de permissões de acesso e metadados de ficheiros
- Adulteração de estruturas de pastas: Modificação maliciosa da hierarquia de organização dos ficheiros

4.4.3 Repudiation (Repúdio)

- Falsificação de operações no sistema de partilha: Execução de ações de partilha com subsequente alteração dos registos para negar responsabilidade
- Repúdio de criação de grupo: Criador de um grupo nega ter adicionado determinados membros com permissões de partilha
- Remoção seletiva de logs de atividade: Eliminação de registos específicos para esconder rastos de acesso não autorizado

4.4.4 Information Disclosure (Divulgação de Informação)

- Acesso não autorizado a ficheiros armazenados: Obtenção de documentos sem as devidas permissões
- Leak de credenciais e perfis de utilizadores: Exposição de nomes de utilizador, senhas ou tokens de autenticação, informações pessoais
- Exposição de chaves criptográficas: Acesso indevido às chaves utilizadas para cifrar e decifrar os dados
- Exposição de metadados sensíveis: Leak de informações sobre documentos, podendo revelar conteúdo confidencial

4.4.5 Denial of Service (Negação de Serviço)

- Bloqueio de acesso a cofres partilhados: Impedimento do acesso a ficheiros críticos em cofres de grupo
- Encriptação maliciosa de ficheiros armazenados: Ransomware que cifra documentos e exige resgate para restauro
- Sabotagem da sincronização de dados: Manipulação que impede a correta sincronização entre dispositivos e servidor
- Saturação do espaço de armazenamento: Upload deliberado de grandes volumes de dados para esgotar o espaço disponível

4.4.6 Elevation of Privilege (Elevação de Privilégio)

- Manipulação de configurações de permissões: Alteração não autorizada dos controlos de acesso para obter privilégios adicionais

- Exploração da permissão de partilha: Uso indevido da capacidade de concessão de permissão para elevar privilégios
- Escalada de privilégios via manipulação de grupos: Contorno de restrições através da exploração da estrutura de grupos

5 Análise de risco das ameaças

5.1 Metodologia

Realizou-se uma análise de risco para entender que ameaças merecem prioridade na fase de desenvolver soluções. Para realizar esta análise de risco, utilizar-se-à a seguinte metodologia:

- Probabilidade (P): Escala de 1 a 5, onde 1 é muito improvável e 5 é quase certo.
- Impacto (I): Escala de 1 a 5, onde 1 é impacto mínimo e 5 é impacto crítico.
- Risco (R): P × I, resultando numa escala de 1-25.
- Classificação de risco:
  - Baixo: 1-4
  - Médio: 5-10
  - Alto: 11-15
  - Crítico: 16-25

5.2 Risco das ameaças ao Servidor

Tabela de Riscos ao Servidor			
Ameaça	Probabilidade	Impacto	Risco
Spoofing			
Interceção de tokens de autenticação	4/5 (Alta)	5/5 (Crítico)	20/25 (Crítico)
Falsificação de convites de grupo	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
IP spoofing em comunicações com microsserviços	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
API endpoint spoofing	2/5 (Média)	5/5 (Crítico)	10/25 (Médio)
Tampering			
Injeção de código em microsserviços	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
SQL injection	4/5 (Alta)	5/5 (Crítico)	20/25 (Crítico)
Comprometimento do middleware de autorização	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Manipulação de payloads JSON	4/5 (Alta)	4/5 (Alto)	16/25 (Crítico)
Repudiation			
Desativação seletiva de logs nos microsserviços	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Adulteração do sistema de monitorização	2/5 (Baixa)	4/5 (Alto)	8/25 (Médio)
Manipulação de logs do PostgreSQL e Nginx	2/5 (Baixa)	4/5 (Alto)	8/25 (Médio)
Mask de tráfego entre microsserviços	2/5 (Baixa)	3/5 (Médio)	6/25 (Médio)
Information Disclosure			
Exposição de dados via falhas nos microsserviços	4/5 (Alta)	5/5 (Crítico)	20/25 (Crítico)
Exploração de vulnerabilidades no PostgreSQL	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Sniffing em endpoints de API não protegidos	4/5 (Alta)	4/5 (Alto)	16/25 (Crítico)

Leak através de cabeçalhos HTTP	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Denial of Service			
Ataques DDoS a microsserviços críticos	4/5 (Alta)	4/5 (Alto)	16/25 (Crítico)
Saturação do PostgreSQL	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
API rate limiting bypass	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Elevation of Privilege			
Exploração de falhas no middleware de autorização	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Bypass da camada de autorização	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Escalada horizontal entre microsserviços	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Exploração de configurações incorretas do Nginx	3/5 (Média)	4/5 (Alto)	12/25 (Alto)

5.3 Risco das ameaças ao Serviço Web

Tabela de Riscos ao Serviço Web			
Ameaça	Probabilidade	Impacto	Risco
Spoofing			
Phishing direcionado via replicação do serviço web	4/5 (Média)	5/5 (Crítico)	20/25 (Crítico)
DNS cache poisoning no acesso ao serviço web	2/5 (Baixa)	5/5 (Crítico)	10/25 (Médio)
Tampering			
Adulteração de cabeçalhos HTTP	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Man-in-the-middle em PWA-servidor	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Information Disclosure			
Análise de tráfego criptografado	2/5 (Baixa)	3/5 (Médio)	6/25 (Médio)
Interseção de credenciais em conexões não-TLS	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Elevation of Privilege			
Manipulação do protocolo de autenticação	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)

5.4 Risco das ameaças à Aplicação Móvel

Tabela de Riscos à Aplicação Móvel			
Ameaça	Probabilidade	Impacto	Risco
Spoofing			
Bluetooth address spoofing	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Tampering			
Injeção de código durante sincronização offline	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Adulteração da PWA em cache	2/5 (Baixa)	5/5 (Crítico)	10/25 (Médio)
Interseção de comunicações Bluetooth	3/5 (Média)	4/5 (Médio)	12/25 (Alto)
Repudiation			

Negação de transferência via Bluetooth	3/5 (Média)	2/5 (Baixo)	6/25 (Médio)
Information Disclosure			
Leak de informação via cache da PWA	4/5 (Média)	5/5 (Crítico)	20/25 (Crítico)
Denial of Service			
Bloqueio de sincronização	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Ataques ao sistema Bluetooth	2/5 (Baixa)	2/5 (Baixo)	4/25 (Baixo)

5.5 Risco das ameaças aos Dados

Tabela de Riscos aos Dados			
Ameaça	Probabilidade	Impacto	Risco
Spoofing			
Falsificação de propriedade na partilha de ficheiros	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Falsificação de metadados de autoria	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Manipulação de identificadores de grupo	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Tampering			
Modificação indevida de ficheiros armazenados	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Corrupção da base de dados PostgreSQL	2/5 (Baixa)	5/5 (Crítico)	10/25 (Médio)
Adulteração de estruturas de pastas	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Repudiation			
Falsificação de operações no sistema de partilha	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Repúdio de criação de grupo	3/5 (Média)	3/5 (Médio)	9/25 (Médio)
Remoção seletiva de logs de atividade	2/5 (Baixa)	4/5 (Alto)	8/25 (Médio)
Information Disclosure			
Acesso não autorizado a ficheiros armazenados	4/5 (Alta)	5/5 (Crítico)	20/25 (Crítico)
Leak de credenciais e perfis de utilizadores	4/5 (Alta)	5/5 (Crítico)	20/25 (Crítico)
Exposição de chaves criptográficas	4/5 (Média)	5/5 (Crítico)	20/25 (Crítico)
Exposição de metadados sensíveis	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Denial of Service			
Bloqueio de acesso a cofres partilhados	3/5 (Média)	4/5 (Alto)	12/25 (Alto)
Encriptação maliciosa de ficheiros armazenados	2/5 (Média)	5/5 (Crítico)	10/25 (Médio)
Sabotagem da sincronização de dados	3/5 (Média)	3/5 (Média)	9/25 (Média)
Saturação do espaço de armazenamento	4/5 (Alta)	3/5 (Médio)	12/25 (Alto)
Elevation of Privilege			
Manipulação de configurações de permissões	3/5 (Média)	5/5 (Crítico)	15/25 (Alto)
Exploração da permissão de partilha	4/5 (Alta)	4/5 (Alto)	16/25 (Crítico)
Escalada de privilégios via manipulação de grupos	3/5 (Média)	4/5 (Alto)	12/25 (Alto)

6 Requisitos de segurança e sugestões de resposta

Com base na análise de riscos realizada para o sistema de Cofre Digital, foram identificados os requisitos de segurança críticos, juntamente com sugestões de resposta técnicas para mitigar cada risco.

6.1 Requisitos de Segurança para o Servidor

6.1.1 Proteção Robusta contra Interceção de Tokens de Autenticação (20/25)

O sistema deve implementar mecanismos para proteger os tokens de autenticação contra interceção durante o trânsito e armazenamento. Sugestões de Resposta:

- Implementar tokens JWT (JSON Web Tokens) com assinatura e cifra
- Implementar tempos de expiração para tokens de acesso (15-30 minutos) e rotação e invalidação em caso de suspeita
- Transmitir tokens apenas através de canais cifrados (TLS 1.3)

6.1.2 Proteção contra SQL Injection (20/25)

O sistema deve implementar defesas robustas contra ataques de injeção SQL em todos os pontos de acesso à base de dados PostgreSQL. Sugestões de Resposta:

- Utilizar consultas parametrizadas ou prepared statements exclusivamente
- Implementar ORM (Object-Relational Mapping) com validação rigorosa
- Aplicar princípio de privilégio mínimo nas contas de acesso à BD
- Implementar filtragem e sanitização de entrada de dados em várias camadas
- Utilizar validação baseada em *schema* para todas as entradas

6.1.3 Proteção contra Manipulação de Payloads JSON (16/25)

O sistema deve prevenir a manipulação maliciosa de payloads JSON nas comunicações entre componentes do sistema. Sugestões de Resposta:

- Implementar validação rigorosa baseada em esquemas (JSON Schema) para todos os payloads
- Utilizar assinaturas digitais para garantir integridade dos payloads
- Controlar tipos de dados e valores permitidos
- Implementar mecanismos anti-replay para evitar ataques de repetição

6.1.4 Proteção contra Exposição de Dados via Falhas nos Microsserviços (20/25)

O sistema deve implementar mecanismos para prevenir a exposição não intencional de dados através de falhas na arquitetura de microsserviços. Sugestões de Resposta:

- Implementar isolamento rigoroso entre microsserviços usando namespaces e políticas de rede
- Utilizar API Gateway com validação de entrada centralizada
- Aplicar princípio de privilégio mínimo para comunicações entre serviços
- Desenvolver controlo granular de acesso a dados entre microsserviços
- Realizar auditorias de configuração automatizadas

6.1.5 Proteção contra Sniffing em Endpoints de API Não Protegidos (16/25)

O sistema deve proteger todas as comunicações API contra interceção e análise não autorizada. Sugestões de Resposta:

- Implementar TLS 1.3 com configuração segura em todos os endpoints
- Utilizar HSTS (HTTP Strict Transport Security) para forçar conexões seguras
- Inspecionar e validar certificados em ambos os lados da comunicação
- Implementar verificação de integridade de mensagens

- Realizar monitorização contínua de tráfego não cifrado
- Utilizar comunicação sobre canais cifrados para transferência de dados entre microsserviços

6.1.6 Proteção contra Ataques DDoS a Microsserviços Críticos (16/25)

O sistema deve implementar proteções contra ataques de negação de serviço distribuído que possam comprometer a disponibilidade. Sugestões de Resposta:

- Implementar limitação de taxa (rate limiting) em todas as APIs
- Implementar autoscaling automático baseado em carga
- Implementar monitorização de tráfego com alertas para padrões anômalos
- Implementar mecanismos de *graceful degradation* para manter funcionalidades críticas

6.1.7 Proteção contra Falsificação de convites de grupo (12/25)

O sistema deve validar a autenticidade dos convites para evitar que utilizadores recebam convites falsos ou adulterados. Sugestões de Resposta:

- Gerar convites com tokens únicos e data de expiração.
- Verificar no backend se o remetente está autorizado e se o token corresponde ao grupo em questão.

6.1.8 Proteção contra IP spoofing em comunicações com microsserviços (12/25)

O sistema deve impedir que endereços IP sejam falsificados nas trocas de dados entre serviços. Sugestões de Resposta:

- Utilizar mTLS (autenticação mútua) e cabeçalhos de encaminhamento confiáveis.
- Configurar regras de firewall e políticas de rede que restrinjam origens não reconhecidas.

6.1.9 Proteção contra Injeção de código em microsserviços (15/25)

O sistema deve controlar entradas maliciosas que possam injetar comandos ou scripts indevidos. Sugestões de Resposta:

- Sanitizar e validar parâmetros de entrada em cada microsserviço.
- Restringir ou evitar funções que executem código dinâmico e aplicar princípio de mínimo privilégio.

6.1.10 Proteção contra Comprometimento do middleware de autorização (15/25)

O sistema deve preservar a segurança do componente que gere permissões de acesso. Sugestões de Resposta:

- Isolar o middleware em container ou serviço dedicado, com logs de auditoria ativados.
- Validar cuidadosamente qualquer atualização ou alteração de configuração no middleware.

6.1.11 Proteção contra Desativação seletiva de logs nos microsserviços (12/25)

O sistema deve impedir que agentes mal-intencionados desativem ou manipulem a geração de logs. Sugestões de Resposta:

- Exigir permissões elevadas para modificar configurações de logging.
- Enviar registos para um serviço central de logs, com verificação periódica de integridade.

6.1.12 Proteção contra Exploração de vulnerabilidades no PostgreSQL (15/25)

O sistema deve prevenir ataques que explorem falhas ou configurações inseguras na base de dados. Sugestões de Resposta:

- Manter o PostgreSQL sempre atualizado, aplicando correções de segurança.
- Definir regras restritas de acesso (pg_hba.conf) e usar contas com privilégios mínimos.

6.1.13 Proteção contra Saturação do PostgreSQL (12/25)

O sistema deve evitar que a base de dados seja sobrecarregada e negue serviço a outros componentes. Sugestões de Resposta:

- Implementar pool de conexões e limites de requisições simultâneas.
- Monitorizar métricas de desempenho e configurar alertas para uso excessivo de recursos.

6.1.14 Proteção contra Exploração de falhas no middleware de autorização (15/25)

O sistema deve impedir que falhas no middleware abram caminho a acessos não autorizados. Sugestões de Resposta:

- Validar tokens e permissões em cada requisição, não apenas no momento de login.
- Executar testes de penetração focados no fluxo de autorização para identificar lógicas inseguras.

6.1.15 Proteção contra Bypass da camada de autorização (15/25)

O sistema deve bloquear tentativas de contornar as verificações de acesso. Sugestões de Resposta:

- Exigir autenticação e autorização em todos os endpoints críticos, sem exceções.
- Rever permissões e papéis (roles) para garantir que não existam rotas de acesso ocultas.

6.1.16 Proteção contra Escalada horizontal entre microsserviços (15/25)

O sistema deve isolar corretamente cada microsserviço para evitar que o acesso a um leve ao controlo de outro. Sugestões de Resposta:

- Implementar autenticação mútua entre serviços, usando tokens ou certificados exclusivos.
- Separar dados e permissões por microsserviço, adotando políticas de rede (NetworkPolicy) restritivas.

6.1.17 Proteção contra Exploração de configurações incorretas do Nginx (12/25)

O sistema deve minimizar riscos causados por configurações mal definidas no servidor. Sugestões de Resposta:

- Rever regularmente diretivas como redirecionamentos, cabeçalhos de segurança e índices de diretório.
- Restringir métodos HTTP não utilizados e ativar logs de acesso/erro para auditoria.

6.2 Requisitos de Segurança para o Serviço Web

6.2.1 Proteção contra Phishing Direcionado via Replicação do Serviço Web (20/25)

O sistema deve implementar mecanismos para dificultar replicação do serviço web para fins de phishing. Sugestões de Resposta:

- Criar um sistema de notificação para logins de localizações não usuais
- Implementar HSTS (HTTP Strict Transport Security) e listas de preload
- Utilizar CSP (Content Security Policy) para prevenir cross-site scripting

6.2.2 Proteção contra Adulteração de cabeçalhos HTTP (12/25)

O sistema deve impedir a manipulação maliciosa de cabeçalhos que possa comprometer a segurança. Sugestões de Resposta:

- Validar e sanitizar cabeçalhos recebidos, descartando valores suspeitos.
- Utilizar assinaturas ou HMAC em cabeçalhos críticos sempre que possível.

6.2.3 Proteção contra Man-in-the-middle em Web-servidor (15/25)

O sistema deve evitar a interceção de comunicações entre a aplicação web e o servidor. Sugestões de Resposta:

- Forçar HTTPS em todas as rotas e aplicar HSTS (HTTP Strict Transport Security).

6.2.4 Proteção contra Interseção de credenciais em conexões não-TLS (15/25)

O sistema deve garantir que credenciais nunca trafeguem em texto claro. Sugestões de Resposta:

- Recusar conexões em HTTP simples e redirecionar para HTTPS automaticamente.
- Adotar autenticação baseada em tokens ou OAuth 2.0 e invalidar sessões inseguras.

6.2.5 Proteção contra Manipulação do protocolo de autenticação (15/25)

O sistema deve assegurar a integridade do fluxo de login e renovação de tokens. Sugestões de Resposta:

- Empregar métodos seguros de autenticação (ex.: OAuth/OpenID Connect) e tokens não replicáveis.
- Implementar verificação de nonce/estado para prevenir ataques de replay ou CSRF.

6.3 Requisitos de Segurança para a Aplicação Móvel

6.3.1 Proteção contra Leak de Informação via Cache da PWA (20/25)

O sistema deve garantir que dados sensíveis armazenados localmente na PWA sejam devidamente protegidos. Sugestões de Resposta:

- Implementar criptografia local para todos os dados em cache
- Utilizar APIs seguras do navegador como IndexedDB com proteções adicionais
- Utilizar verificação de integridade para dados offline
- Implementar limpeza automática de dados sensíveis em caso de inatividade
- Desenvolver mecanismo de sincronização segura entre cache local e servidor

6.3.2 Proteção contra Injeção de código durante sincronização offline (12/25)

O sistema deve evitar que scripts maliciosos se infiltrem durante o processo de sincronização. Sugestões de Resposta:

- Validar a estrutura dos dados recebidos antes de armazenar localmente.
- Evitar execuções dinâmicas (eval) e reforçar políticas de conteúdo (Content Security Policy).

6.3.3 Proteção contra Interseção de comunicações Bluetooth (12/25)

O sistema deve salvaguardar a troca de dados via Bluetooth, prevenindo interceção ou adulteração. Sugestões de Resposta:

- Aplicar emparelhamento seguro (usando chaves de sessão e criptografia) e verificar identidades.
- Monitorar desconexões e tentativas de reconexão não autorizadas, emitindo alertas ao usuário.

6.4 Requisitos de Segurança para os Dados

6.4.1 Proteção contra Acesso Não Autorizado a Ficheiros Armazenados (20/25)

O sistema deve garantir que ficheiros armazenados não possam ser acessados por utilizadores não autorizados, mesmo em caso de comprometimento parcial do sistema. Sugestões de Resposta:

- Implementar criptografia de ficheiros em repouso
- Utilizar criptografia de envelope com chaves por ficheiro
- Implementar controlo de acesso em várias camadas (aplicação, BD, armazenamento)
- Implementar sistema de deteção de acessos anômalos baseado em comportamento
- Criar políticas de retenção e destruição segura de dados

6.4.2 Proteção contra *Leak* de Credenciais e Perfis de Utilizadores (20/25)

O sistema deve proteger as credenciais e informações de perfil dos utilizadores contra exposição. Sugestões de Resposta:

- Armazenar senhas usando algoritmos de hash seguros
- Isolar dados de perfil em microsserviço dedicado com controlo de acesso restrito
- Implementar princípio de privilégio mínimo para acesso a dados de utilizadores
- Implementar auditorias regulares de acesso a dados de utilizadores

6.4.3 Proteção contra Exposição de Chaves Criptográficas (20/25)

O sistema deve implementar mecanismos robustos para proteger as chaves criptográficas utilizadas para cifrar os dados dos utilizadores. Sugestões de Resposta:

- Implementar um sistema hierárquico de gestão de chaves (Key Management System)
- Implementar rotação automática de chaves com períodos definidos
- Utilizar chaves de derivação diferentes para cada utilizador/cofre
- Utilizar um serviço de gestão de segredos (como AWS KMS, Azure Key Vault) para armazenamento seguro

6.4.4 Proteção contra Exploração da Permissão de Partilha (16/25)

O sistema deve implementar controlos rigorosos que impeçam a exploração indevida dos mecanismos de permissão de partilha. Sugestões de Resposta:

- Implementar um sistema de controlo de acesso baseado em permissões granulares (RBAC/ABAC)
- Implementar auditoria detalhada de todas as operações de partilha
- Desenvolver mecanismos de notificação para o proprietário quando ficheiros são partilhados
- Implementar confirmação adicional para concessão de permissões de repartilha

6.4.5 Proteção contra Falsificação de propriedade na partilha de ficheiros (15/25)

O sistema deve impedir que atores mal-intencionados se façam passar por proprietários de ficheiros. Sugestões de Resposta:

- Associar cada ficheiro a uma assinatura digital do proprietário.
- Validar a autenticidade do remetente sempre que um ficheiro é partilhado ou modificado.

6.4.6 Proteção contra Manipulação de identificadores de grupo (12/25)

O sistema deve proteger os identificadores usados para partilha, evitando fraudes ou acesso indevido. Sugestões de Resposta:

- Gerar identificadores (UUIDs) e validá-los junto às permissões do usuário.
- Não expor lógicas de criação ou detalhes de grupos em parâmetros de URL sem autenticação.

6.4.7 Proteção contra Modificação indevida de ficheiros armazenados (15/25)

O sistema deve detetar e impedir alterações não autorizadas em dados já armazenados. Sugestões de Resposta:

- Manter versionamento de ficheiros e registar histórico de mudanças.
- Usar hashes ou assinaturas digitais para verificar integridade em cada atualização.

6.4.8 Proteção contra Falsificação de operações no sistema de partilha (12/25)

O sistema deve evitar que ações de partilha sejam registadas em nome de outro usuário. Sugestões de Resposta:

- Incluir informações de autenticação na requisição (token) e registar IP/horário do autor.
- Negar operações que não estejam associadas às credenciais corretas ou que apresentem divergências de sessão.

6.4.9 Proteção contra Exposição de metadados sensíveis (12/25)

O sistema deve evitar que informações de contexto (datas, localizações, nomes internos) sejam expostas indevidamente. Sugestões de Resposta:

- Remover metadados de ficheiros (ex.: EXIF) antes de partilhar quando possível.
- Restringir consultas a metadados somente a utilizadores autorizados e auditar acessos.

6.4.10 Proteção contra Bloqueio de acesso a cofres partilhados (12/25)

O sistema deve prevenir bloqueios deliberados de repositórios, negando o acesso a todos os membros legítimos. Sugestões de Resposta:

- Implementar redundância e verificação periódica de disponibilidade dos cofres.
- Limitar tentativas consecutivas de bloqueio e alertar administradores para comportamento anômalo.

6.4.11 Proteção contra Saturação do espaço de armazenamento (12/25)

O sistema deve evitar que utilizadores ou processos excedam a capacidade, prejudicando o acesso de outros. Sugestões de Resposta:

- Atribuir quotas de armazenamento por utilizador ou grupo, com alertas próximos do limite.
- Implementar limpeza periódica de ficheiros temporários e monitorizar crescimento anormal de dados.

6.4.12 Proteção contra Manipulação de configurações de permissões (15/25)

O sistema deve salvaguardar regras de acesso para evitar alterações por utilizadores não autorizados. Sugestões de Resposta:

- Registar todas as mudanças de permissões e exigir privilégios elevados para editá-las.
- Automatizar auditorias frequentes das configurações, reportando qualquer discrepância.

6.4.13 Proteção contra Escalada de privilégios via manipulação de grupos (12/25)

O sistema deve impedir que utilizadores consigam privilégios indevidos alterando grupos ou papéis. Sugestões de Resposta:

- Exigir validação em duas etapas para mudanças de grupos ou inclusão de novos membros com privilégios.
- Armazenar e comparar a hierarquia de grupos em base segura, auditando cada modificação.

7 Conclusão

A análise de risco realizada demonstra que o sistema de Cofre Digital enfrenta diversas ameaças de segurança, classificadas de acordo com sua probabilidade e impacto. Para essa avaliação, utilizámos o modelo STRIDE. Com base nessa avaliação, foram definidos requisitos de segurança críticos e estratégias de mitigação para reduzir as vulnerabilidades identificadas.

A implementação dessas soluções contribuirá significativamente para reforçar a segurança do sistema, protegendo os dados dos utilizadores e garantindo a confiabilidade do serviço. No entanto, a segurança deve ser vista como um processo contínuo, exigindo atualizações regulares, auditorias frequentes e adaptação constante a novas ameaças.

8 Referências

- https://nvd.nist.gov
- https://cve.mitre.org
- https://attack.mitre.org
- https://owasp.org
- https://csrc.nist.gov
- https://cheatsheetseries.owasp.org
- https://infosec.mozilla.org/guidelines/web_security
- https://github.com/OWASP