Universidade do Minho
Escola de Engenharia

Universidade do Minho
Escola de Engenharia
Mestrado em Engenharia Informática

Unidade Curricular de Tecnologias de Segurança

Ano Letivo de 2024/2025

Cofre Digital - TP1 - Grupo 6

Martim Redondo
PG55929

João Rodrigues
PG57879

Benjamim Rodrigues
PG57511

Março, 2025

Índice

Lista de Figuras

Lista de Tabelas

1. Introdução

Nos dias de hoje, a segurança da informação é uma preocupação fundamental para serviços que armazenam e gerem dados sensíveis. Com o avanço da digitalização e da computação em nuvem, garantir a confidencialidade, integridade e disponibilidade dos dados tornou-se um desafio crítico para as empresas e utilizadores. Este trabalho prático tem como objetivo a análise de segurança de um serviço de **Cofre Digital**, que permitirá aos utilizadores armazenar ficheiros de forma segura e partilhá-los com outros utilizadores ou grupos dentro do sistema. O Cofre Digital será composto por três componentes principais: um **servidor**, um **serviço web** e uma **aplicação móvel**, cada um desempenhando um papel fundamental na funcionalidade e segurança do sistema. Para garantir a proteção do sistema, será realizada uma identificação dos principais **ativos do sistema**, para cada ativo descobrir-se-à vulnerabilidades através da aplicação do conceito **STRIDE** para perceber problemas, ameaças iminentes e possíveis mitigações, atribuindo um valor estatístico quando ao risco, impacto e criticidade. Para, no fim, se organizar uma tabela de requisitos. Esta análise será fundamentada em metodologias de segurança amplamente reconhecidas, como **OWASP Threat Modeling, MITRE ATT&CK e Common Weakness Enumeration (CWE)**. Além disso, serão considerados padrões de segurança recomendados para proteção de dados em ambiente de nuvem e sistemas distribuídos. Desta forma, o presente documento apresenta uma abordagem sistemática para fortalecer a segurança do Cofre Digital, reduzindo vulnerabilidades e garantindo um ambiente fiável para o armazenamento e partilha de informações sensíveis.

2. Descrição do Sistema

O Cofre Digital é um sistema concebido para permitir o armazenamento seguro e a partilha de ficheiros entre utilizadores e grupos. O sistema é composto por três componentes principais:

2.1. Servidor

O servidor é responsável pela lógica central do sistema, incluindo:

- Registo e autenticação de utilizadores;
- Controlo de acesso a ficheiros e pastas;
- Armazenamento seguro de ficheiros;
- Criação e gestão de grupos e pastas.

O sistema será implementado utilizando uma arquitetura baseada em microsserviços, garantindo escalabilidade e eficiência. Além disso, será hospedado numa infraestrutura de computação em nuvem, assegurando fiabilidade e redundância.

2.2. Serviços Web

O serviço web permite que os utilizadores acedam ao Cofre Digital através de um navegador. As funcionalidades principais incluem:

- Registo e autenticação de utilizadores;
- Gestão de cofres e ficheiros;
- Partilha de ficheiros e pastas com utilizadores e grupos;
- Administração de permissões de acesso.

A comunicação entre o serviço web e o servidor será protegida através de protocolos encriptados, garantindo a segurança dos dados transmitidos.

2.3. Aplicação Móvel

- Suporte para modo offline, permitindo o acesso aos ficheiros mesmo sem conexão à internet;
- Transferência direta de ficheiros entre dispositivos móveis através de Bluetooth, sem necessidade de conexão ao servidor.

O sistema foi concebido com foco na segurança e privacidade, garantindo que apenas utilizadores autorizados tenham acesso aos seus ficheiros e dados pessoais.

3. Modelação de Sistema

3.1. Data Flow Diagram

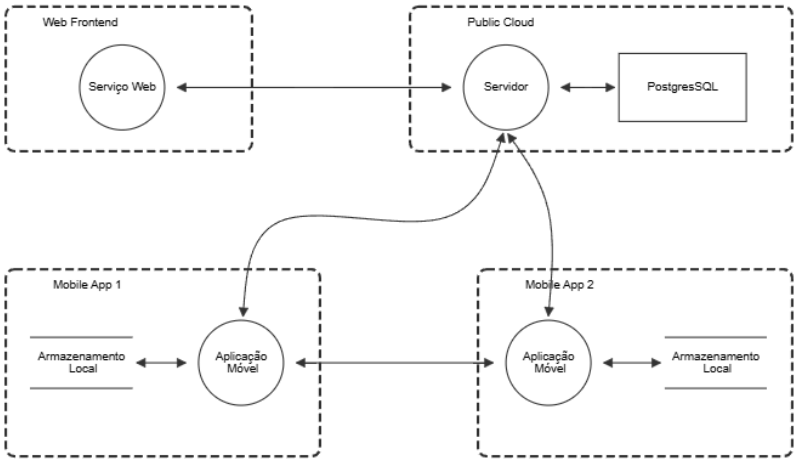

Figura 1: Modelo DFD

O **Data Flow Diagram (DFD)** ilustra a estrutura do Cofre Digital, destacando os fluxos de dados entre os seus principais componentes e os limites de confiança que delimitam diferentes áreas de segurança.

O sistema é dividido em três principais *trust boundaries*. O primeiro, *Web Frontend*, contém o Serviço Web, que serve como interface para os utilizadores acederem ao sistema. Este comunica bilateralmente com o Servidor, localizado dentro do Public Cloud, que centraliza a lógica do serviço e armazena informações no **PostgreSQL**, garantindo persistência e integridade dos dados.

A interação com dispositivos móveis ocorre dentro dos *trust boundaries* Mobile App 1 e Mobile App 2, que representam diferentes instâncias da aplicação em dispositivos distintos. Cada aplicação móvel pode comunicar-se diretamente com o Servidor, permitindo a sincronização de ficheiros e gestão de cofres. Além disso, há um fluxo de dados direto entre duas aplicações móveis, refletindo a funcionalidade de transferência direta de ficheiros via Bluetooth, garantindo disponibilidade mesmo em cenários offline.

O diagrama destaca a separação dos diferentes domínios de confiança para refletir o risco de ataques em cada camada. A comunicação entre os componentes deve ser protegida, garantindo confidencialidade e integridade dos dados armazenados e transmitidos.

3.2. Diagrama de Estados

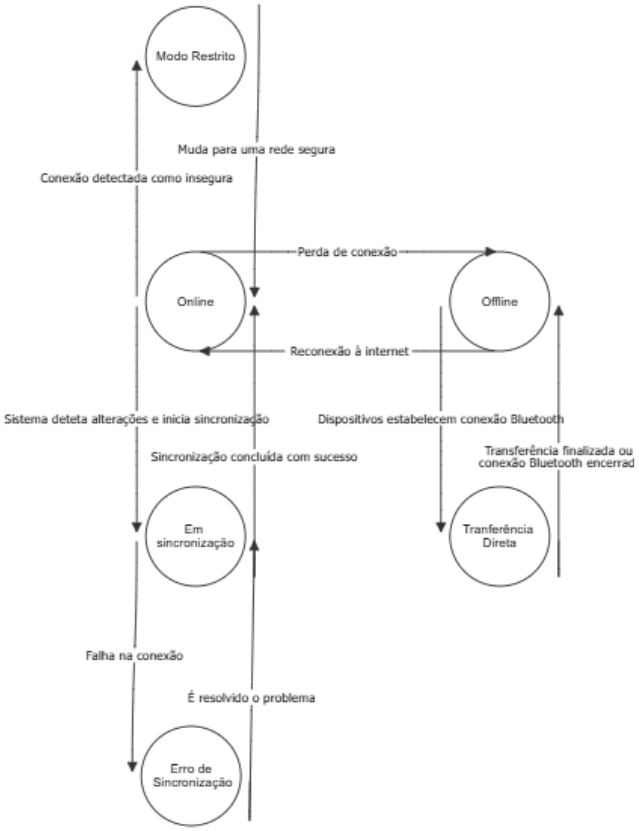

Figura 2: Diagrama de Estados

O diagrama de estados representa o comportamento do Cofre Digital, focando na alternância entre os estados online e offline, bem como em estados intermediários que refletem transições e condições especiais do sistema.

O sistema pode estar em Online, quando tem conexão com o servidor e pode sincronizar dados, ou Offline, quando não há conexão e apenas os dados locais estão acessíveis. Sempre que a conexão é restabelecida, o sistema passa para o estado Em Sincronização, onde os ficheiros locais são comparados com os do servidor para garantir atualizações. Se houver falhas, como conflitos de versões ou problemas de rede, o estado Erro de Sincronização é acionado, exigindo intervenção do utilizador para resolver inconsistências.

Além disso, existe o Modo Restrito, ativado quando o sistema deteta uma conexão insegura (por exemplo, uma rede Wi-Fi pública sem criptografia). Nesse estado, certas funcionalidades podem ser limitadas para evitar riscos à segurança. Outro estado relevante é a Transferência Direta, que ocorre quando dois dispositivos trocam ficheiros via Bluetooth sem necessidade de conexão com o servidor. Após a transferência, o sistema retorna ao estado Offline ou Online, dependendo da conectividade do momento.

As transições entre esses estados refletem as diferentes condições de funcionamento do Cofre Digital, garantindo que os ficheiros permaneçam protegidos e acessíveis mesmo em cenários de falha de rede ou restrições de segurança.

4. Identificação de Ativos

A segurança do Cofre Digital depende da proteção dos seus ativos mais críticos. Nesta secção, serão identificados os principais ativos do sistema e analisadas as ameaças que podem comprometer a sua segurança.

Para isto foi realizada uma modelação de ameaças baseada no modelo **STRIDE** para cada Ativo, identifica-se possíveis fraquezas, ameaças e atribui-se um valor estatístico a cada fraqueza, tendo em conta o seu risco, impacto e criticidade.

4.1. Serviço Web

4.1.1. Modelação de ameaças orientadas ao Software

4.1.1.1. Spoofing

- **Fraquezas**:
  1. A ausência de verificação adequada dos *tokens* de sessão pode permitir que atacantes se passem por utilizadores legítimos;
  2. Sem MFA, uma única credencial comprometida pode ser suficiente para um atacante se passar por um utilizador legítimo;
  3. A falta de confirmação de endereços de e-mail pode ser explorada por atacantes para criar contas fraudulentas.

- **Ameaças**:
  - O atacante pode utilizar um *token* de sessão comprometido para se passar por um utilizador legítimo e aceder ao Cofre Digital sem necessidade de credenciais adicionais;
  - O atacante pode explorar a ausência de *MFA* para comprometer contas usando credenciais roubadas ou obtidas por meio de ataques de força bruta;
  - O atacante pode enganar os utilizadores ao se passar por fontes confiáveis e obter informações sensíveis como senhas.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.1	4/5	5/5	9/10
Fraq.2	5/5	5/5	10/10
Fraq.3	3/5	2/5	5/10

Tabela 1: Analise de Risco - Spoofing - Serviço Web

4.1.1.2. Tampering

- **Fraquezas**:
  1. Sem verificações de integridade, utilizadores com más intenções podem substituir arquivos legítimos por versões comprometidas, prejudicando a confiança nos dados armazenados.
  2. A ausência de mecanismos robustos de controlo de acesso permite que utilizadores acedam ou modifiquem dados para os quais não tem autorização, comprometendo a integridade do sistema.
  3. Sem a devida validação, dados fornecidos por utilizadores maliciosos podem ser processados, levando à alteração ou corrupção de dados sensíveis.
- **Ameaças**:
  - O atacante pode substituir ficheiros legítimos por versões comprometidas.
  - O atacante pode explorar permissões incorretas para modificar ou apagar dados sensíveis sem autorização.
  - O atacante pode enviar dados maliciosos que não são devidamente validados, resultando em corrupção ou alteração indevida de informações no Cofre Digital.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.4	4/5	5/5	9/10
Fraq.5	4/5	5/5	9/10
Fraq.6	3/5	4/5	7/10

Tabela 2: Analise de Risco - Tampering - Serviço Web

4.1.1.3. Repudiation

- **Fraquezas**:
  1. Sem *logs* abrangentes que documentem todas as ações dos usuários, é impossível verificar a autenticidade de operações, tornando o sistema vulnerável a negações de ações realizadas.
  2. Sem políticas claras que restrinjam ações com base em *roles* ou permissões, utilizadores podem realizar operações além de suas autorizações, complicando a responsabilização.

3. A ausência de autenticação robusta permite que atacantes se façam passar por outros utilizadores, dificultando a atribuição de ações específicas a indivíduos reais.

- **Ameaças**:
  - O atacante pode negar ter realizado ações maliciosas, como modificações de dados ou operações críticas, devido à ausência de *logs* abrangentes que registrem essas atividades.
  - O atacante pode explorar permissões excessivas ou mal definidas para realizar ações indevidas e evitar responsabilização.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.7	4/5	5/5	9/10
Fraq.8	3/5	4/5	7/10
Fraq.9	3/5	4/5	7/10

Tabela 3: Analise de Risco - Repudiation - Serviço Web

4.1.1.4. Information Disclosure

- **Fraquezas**:
  1. Mensagens de erro que fornecem informações excessivas sobre a estrutura interna do sistema podem auxiliar atacantes na identificação de vulnerabilidades a serem exploradas.
  2. Configurações de permissões que permitem que usuários não autorizados acessem ou visualizem dados sensíveis podem resultar em divulgação não intencional de informações.
  3. A falta de controle sobre os metadados associados a ficheiros pode revelar informações confidenciais, como autores, datas de criação ou alterações, comprometendo a privacidade dos dados.

- **Ameaças**:
  - O atacante pode aceder a dados sensíveis devido a permissões incorretas, resultando em divulgação não autorizada de informações críticas.
  - O atacante pode analisar metadados associados a ficheiros para obter informações confidenciais, como autores, datas de criação e alterações, comprometendo a privacidade dos utilizadores.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.10	2/5	3/5	5/10
Fraq.11	3/5	4/5	7/10
Fraq.12	3/5	4/5	7/10

Tabela 4: Analise de Risco - Information Disclosure - Serviço Web

4.1.1.5. Denial of Service (DoS)

- **Fraquezas**: :
  1. A ausência de medidas de segurança específicas, como limitação de taxa de pedidos e detecão de padrões anómalos de tráfego, pode deixar o Cofre Digital vulnerável a ataques DoS direcionados.
  2. Sem sistemas de monitorização eficazes, é difícil detectar e responder rapidamente a ataques DoS, permitindo que eles causem danos significativos.

3. A ausência de configurações adequadas de firewall e roteadores pode permitir que tráfego malicioso atinja diretamente os servidores, facilitando ataques DoS.
4. A infraestrutura do sistema pode não suportar picos de tráfego inesperados, tornando-se vulnerável a ataques de sobrecarga.

- **Ameaças**:
  - O atacante pode realizar um ataque DoS enviando um volume excessivo de pedidos, explorando a falta de limitação de taxa e comprometendo a disponibilidade do serviço.
  - O atacante pode direcionar tráfego malicioso diretamente aos servidores devido à configuração inadequada de firewall, aumentando a vulnerabilidade a ataques DoS.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.13	4/5	5/5	9/10
Fraq.14	3/5	4/5	7/10
Fraq.15	3/5	4/5	7/10
Fraq.16	4/5	5/5	9/10

Tabela 5: Analise de Risco - Denial of Service - Serviço Web

4.1.1.6. Elevation of Privilege

- **Fraquezas**:
1. Se o sistema não verificar corretamente as permissões de cada utilizador ao aceder a recursos sensíveis, um utilizador com privilégios limitados pode obter acesso não autorizado a funcionalidades restritas.
2. A ausência de registos detalhados e monitorização das atividades dos utilizadores pode dificultar a deteção de tentativas de elevação de privilégios, permitindo que atacantes mantenham acesso elevado sem serem identificados.
3. Se as sessões não forem geridas de forma segura, como a utilização de identificadores de sessão previsíveis ou a falta de expiração de sessões inativas, um atacante pode sequestrar uma sessão legítima e obter privilégios elevados.

- **Ameaças**:
  - O atacante pode explorar a falta de verificação de permissões para aceder a funcionalidades ou recursos restritos, obtendo privilégios superiores aos autorizados.
  - O atacante pode manter privilégios elevados sem ser detetado devido à ausência de registos detalhados e monitorização das atividades dos utilizadores.
  - O atacante pode sequestrar sessões legítimas, caso estas não sejam geridas de forma segura, e obter acesso com privilégios elevados.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.17	4/5	5/5	9/10
Fraq.18	2/5	3/5	5/10
Fraq.19	3/5	4/5	7/10

Tabela 6: Analise de Risco - Elevation of Privilege - Serviço Web

4.2. Servidor

4.2.1. Análise geral de riscos

O servidor compõe o núcleo do serviço de **Cofre Digital** utilizando **Fedora Server 41** como sistema operativo, **Nginx 1.24.0** como servidor web (responsável pelo tráfego e segurança da comunicação) e **PostgreSQL 10.22** para armazenar dados críticos.

Numa primeira análise há o realçar de alguns problemas como:

- Uso de uma versão antiga do **PostgreSQL**, que terá vulnerabilidades já descobertas expostas;
- Uso de **Fedora Server 41** uma versão muito recente e com pouca análise de vulnerabilidades, podendo surgir um novo problema numa frequência maior, aquando comparado com versões mais estáveis.

Apesar de haver problemas com o uso destas tecnologias, também, é de realçar o facto de que todas as vulnerabilidades descobertas são solucionadas no máximo 2/3 semanas, ou seja, mesmo com o surgimento de problemas há a garantia de que a mitigação surgirá num tempo curto.

4.2.2. Modelação de ameaças orientadas ao Software

4.2.2.1. Spoofing

- **Fraquezas**:
  1. Uso das ferramentas do **Fedora Server**, *Pluggable Authentication Modules* (PAM), de forma pouco robusta;
  2. Inexistência de políticas de senha fortes;
  3. Quanto ao uso de **Nginx**, mau gerenciamento das chaves e certificados;
  4. Mau controle sobre a segurança de autenticação entre microsserviços.
- **Ameaças**:
  - O atacante pode conseguir acesso a contas com credencias fracas;
  - O atacante pode conseguir falsificar um serviço legítimo.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.20	3/5	3/5	6/10
Fraq.21	4/5	4/5	8/10
Fraq.22	4/5	3/5	7/10
Fraq.23	4/5	5/5	9/10

Tabela 7: Analise de Risco - Spoofing - Servidor

4.2.2.2. Tampering

- **Fraquezas**:
  1. Ataques de **Man-in-the-middle** caso não haja uma comunicação completamente encriptada;
  2. Ausência de mecanismos de integridade para ficheiros e logs.

3. Devido ao **PostfreSQL** ser uma versão antiga e não poder ser atualizada devido às exigências do serviço, há vulnerabilidades expostas.

- **Ameaças**:
  - O atacante pode mudar informações/dados colocando-se no meio da comunicação. O
  - O que pode acontecer, também, devido ao uso de versões precárias de estruturas de armazenamento de dados é a modificação do sistema através de comandos arbitrários (**CVE-2019-9193** - afeta versões entre 9.3 até 11.2).

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.24	4/5	4/5	8/10
Fraq.25	3/5	3/5	6/10
Fraq.26	4/5	5/5	9/10

Tabela 8: Analise de Risco - Tampering - Servidor

4.2.2.3. Repudiation

- **Fraquezas**:
  1. Má configuração do **Fedora 41** no registo de eventos;
  2. Falta de logs estruturalmente bem organizados aquando do uso de **Nginx** e **PostgreSQL**.

- **Ameaças**: -O utilizador pode negar ações realizadas, essas ações podem ser atividades maliciosas ou erros críticos, o que leva a ser difícil atribuir culpas, descobrir o erro e até corrigi-lo.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.27	3/5	3/5	6/10
Fraq.28	3/5	4/5	7/10

Tabela 9: Analise de Risco - Repudiation - Servidor

4.2.2.4. Information Disclosure

- **Fraquezas**:
  1. Exposição de cabeçalhos e informações de versão e, nos piores casos, de diretórios sensíveis;
  2. Acesso indesejado a dados em repouso;
  3. Má configuração de mensagens de erro/debug, pois podem revelar detalhes cruciais sobre o funcionamento interno do servidor.

- **Ameaças**:
  - Acesso indevido a informação, ou obtenção de informação de forma despretensiosa.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.29	3/5	3/5	6/10
Fraq.30	4/5	4/5	8/10
Fraq.31	3/5	3/5	6/10

Tabela 10: Analise de Risco - Information Disclosure - Servidor

4.2.2.5. Denial of service

- **Fraquezas**:
  1. Vulnerável a ataques DoS (sobrecarga do serviço de rede) devido ao mau uso da tecnologia **Nginx**;
  2. Vulnerável a ataques que visam preencher o bando de dados **PostgreSQL**.
- **Ameaças**:
  - Indisponibilidade do serviço;
  - lentidão ou bloqueio de acesso a dados críticos.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.32	4/5	4/5	8/10
Fraq.33	3/5	4/5	7/10

Tabela 11: Analise de Risco - Denial of service - Servidor

4.2.2.6. Elevation of Privilege

- **Fraquezas**:
  1. O **Fedora** não estiver configurado para aplicar o princípio do **menor privilégio** (todos os utilizadores começam com 0 privilégios dentro do sistema);
  2. O **Fedora** não tiver os serviços, corretamente, isolados.
  3. Possibilidade de haver um *endpoint* exposto sem verificações rigorosas;
  4. o uso do próprio **PostgreSQL** torna-se uma ameaça.
- **Ameaças**:
  1. Exploração as falhas do **Fedora** para obter privilégios elevados;
  2. Manipulação de parâmetros no *endpoint*, de maneira a conseguir acessar funcionalidades administrativas;
  3. Vulnerabilidade no **PostgreSQL** devido à versão (**CVE-2019-9193** - afeta versões entre 9.3 até 11.2) permite ao atacante executar com privilégios elevados no sistema operacional.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.34	4/5	4/5	8/10
Fraq.35	4/5	4/5	8/10
Fraq.36	4/5	5/5	9/10
Fraq.37	4/5	5/5	9/10

Tabela 12: Analise de Risco - Elevation of Privilege - Servidor

4.3. Aplicação móvel

4.3.1. Modelação de ameaças orientadas ao Software

4.3.1.1. Spoofing

- **Fraquezas**:

1. Armazenamento inseguro de credenciais do utilizador

2. Falta de autenticação forte para atualização de dados.

- **Ameaças**:
  - Um atacante pode tentar aceder à conta de outro utilizador explorando vulnerabilidades na autenticação.
  - Se as credenciais forem armazenadas em texto simples ou com hashing fraco, podem ser comprometidas e utilizadas para obter acesso não autorizado.
  - A ausência de um mecanismo de autenticação forte nas atualizações pode permitir que um atacante se faça passar pelo servidor para injetar código malicioso.
- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.38	5/5	5/5	10/10
Fraq.39	5/5	5/5	10/10

Tabela 13: Analise de Risco - Spoofing - Aplicação móvel

4.3.1.2. Tampering

- **Fraquezas**:

1. Alteração não autorizada do código da aplicação
2. Alteração não autorizada dos ficheiros locais.

- **Ameaças**:
  - Um atacante pode modificar a aplicação para desativar medidas de segurança, instalar backdoors ou injetar código malicioso.
  - Ficheiros armazenados localmente podem ser adulterados, comprometendo a integridade dos dados.
- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.40	5/5	5/5	10/10
Fraq.41	5/5	5/5	10/10

Tabela 14: Analise de Risco - Tampering - Aplicação móvel

4.3.1.3. Repudiation

- **Fraquezas**:

1. Falta de mecanismos de registo e auditoria.

- **Ameaças**:
  - Um utilizador pode negar a execução de uma ação, alegando que não foi ele a realizar determinada operação.
- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.42	4/5	4/5	8/10

Tabela 15: Analise de Risco - Repudiation - Aplicação móvel

4.3.1.4. Information Disclosure

- **Fraquezas**:

1. Exposição de dados sensíveis devido a armazenamento inseguro
2. Exposição de dados sensíveis devido a transmissão desprotegida.

- **Ameaças**:
  - Um atacante pode obter acesso a dados privados do utilizador ao explorar falhas na encriptação ou armazenamento local.

- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.43	5/5	5/5	10/10
Fraq.44	5/5	5/5	10/10

Tabela 16: Analise de Risco - Information Disclosure - Aplicação móvel

4.3.1.5. Denial of service

- **Fraquezas**:

1. Falta de limitação de requisições
2. Falta de proteção contra sobrecarga.

- **Ameaças**:
  - Um atacante pode sobrecarregar a aplicação através de requisições excessivas, tornando-a indisponível.

- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.45	2/5	4/5	6/10
Fraq.46	3/5	4/5	7/10

Tabela 17: Analise de Risco - Denial of service - Aplicação móvel

4.3.1.6. Elevation of Privilege

- **Fraquezas**:

1. Permissões mal configuradas podem conceder privilégios indevidos a utilizadores não autorizados.

- **Ameaças**:
  - Um utilizador malicioso pode explorar falhas na gestão de permissões para realizar ações restritas.

- **Análise de Risco**:

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.47	5/5	5/5	10/10

Tabela 18: Analise de Risco - Elevation of Privilege - Aplicação móvel

4.4. Comunicação

4.4.1. Modelação de ameaças orientadas ao Software

4.4.1.1. Spoofing

- **Fraquezas**:
  1. Falta de autenticação forte entre os componentes do sistema pode permitir que atacantes se passem por entidades legítimas.
- **Ameaças**:
  - Um atacante pode se fazer passar pelo servidor ou pelo cliente, capturando dados sensíveis ou enviando informações maliciosas.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.48	4/5	5/5	9/10

Tabela 19: Analise de Risco - Spoofing - Comunicação

4.4.1.2. Tampering

- **Fraquezas**:
  1. Falta de mecanismos para garantir a integridade das mensagens trocadas entre os componentes do sistema.
- **Ameaças**:
  - Um atacante pode modificar pacotes de dados em trânsito, alterando comandos ou informações transmitidas.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.49	4/5	4/5	8/10

Tabela 20: Analise de Risco - Tampering - Comunicação

4.4.1.3. Repudiation

- **Fraquezas**:
  1. Ausência de logs detalhados;
  2. Ausência de assinaturas digitais para rastrear as comunicações.
- **Ameaças**:
  - Um utilizador mal-intencionado pode negar ter enviado ou recebido determinadas mensagens.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.50	3,5	4,5	7,10
Fraq.51	4/5	5/5	9/10

Tabela 21: Analise de Risco - Repudiation - Comunicação

4.4.1.4. Information Disclosure

- **Fraquezas**:
  1. Falhas na criptografia da comunicação podem expor dados sensíveis a terceiros.
- **Ameaças**:
  - Um atacante pode capturar comunicações não protegidas, obtendo informações confidenciais dos utilizadores.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.52	3/5	3/5	6/10

Tabela 22: Analise de Risco - Information Disclosure - Comunicação

4.4.1.5. Denial of service

- **Fraquezas**:
  1. Falta de proteção contra picos anormais de tráfego pode comprometer a disponibilidade do serviço.
- **Ameaças**:
  - Um atacante pode sobrecarregar o sistema com requisições massivas, impedindo o funcionamento normal.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.53	4/5	4/5	8/10

Tabela 23: Análise de Risco - Denial of service - Comunicação

4.4.1.6. Elevation of Privilege

- **Fraquezas**:
  1. Falhas nos mecanismos de autenticação podem permitir que um atacante obtenha permissões indevidas.
- **Ameaças**:
  - Um utilizador com privilégios baixos pode explorar vulnerabilidades no sistema de comunicação para executar ações restritas.

Fraqueza_ID	Risco	Impacto	Criticidade
Fraq.54	4/5	5/5	9/10

Tabela 24: Analise de Risco - Elevation of Privilege- Comunicação

5. Requisitos de Segurança

A tabela abaixo irá conter, unicamente, as fraquezas mais importantes a serem tratadas, ou seja, aquelas que envolvem um risco maior.

Fraqueza_ID	Criticidade	Fraqueza
1	9	A ausência de verificação adequada dos *tokens* de sessão pode permitir que atacantes se passem por utilizadores legítimos
2	10	Sem MFA, uma única credencial comprometida pode ser suficiente para um atacante se passar por um utilizador legítimo
4	9	O atacante pode explorar permissões incorretas para modificar ou apagar dados sensíveis sem autorização
5	9	O atacante pode enviar dados maliciosos que não são devidamente validados, resultando em corrupção ou alteração indevida de informações no Cofre Digital
7	9	A ausência de autenticação robusta permite que atacantes se façam passar por outros utilizadores, dificultando a atribuição de ações específicas a indivíduos reais
13	9	A ausência de medidas de segurança específicas, como limitação de taxa de pedidos e detecão de padrões anómalos de tráfego, pode deixar o Cofre Digital vulnerável a ataques DoS direcionados
16	9	A infraestrutura do sistema pode não suportar picos de tráfego inesperados, tornando-se vulnerável a ataques de sobrecarga
17	9	Se o sistema não verificar corretamente as permissões de cada utilizador ao aceder a recursos sensíveis, um utilizador com privilégios limitados pode obter acesso não autorizado a funcionalidades restritas
21	8	Inexistência de políticas de senha fortes
23	9	Mau controle sobre a segurança de autenticação entre microsserviços
26	9	Devido ao **PostfreSQL** ser uma versão antiga e não poder ser atualizada devido às exigências do serviço, há vulnerabilidades expostas.
36	9	Possibilidade de haver um *endpoint* exposto sem verificações rigorosas
37	9	O uso do próprio **PostgreSQL** torna-se uma ameaça
38	10	Armazenamento inseguro de credenciais do utilizador
39	10	Falta de autenticação forte para atualização de dados
40	10	Alteração não autorizada do código da aplicação
41	10	Alteração não autorizada dos ficheiros locais
43	10	Exposição de dados sensíveis devido a armazenamento inseguro
44	10	Exposição de dados sensíveis devido a transmissão desprotegida
47	10	Permissões mal configuradas podem conceder privilégios indevidos a utilizadores não autorizados
48	9	Falta de autenticação forte entre os componentes do sistema pode permitir que atacantes se passem por entidades legítimas
51	9	Ausência de assinaturas digitais para rastrear as comunicações
54	9	Falhas nos mecanismos de autenticação podem permitir que um atacante obtenha permissões indevidas

Tabela 25: Requisitos de Segurança

6. Mitigação dos problemas

Fraqueza_ID	Mitigação
1, 2	Implementar autenticação multifator (**MFA**), comunicação segura via **TLS** e gestão eficaz de sessões com *tokens* temporários
4, 5	Utilizar validações rigorosas de entrada, assinaturas digitais, *hashes* criptográficos e controlos de acesso robustos
7	Implementar *logs* detalhados e imutáveis, assinaturas digitais e análise automática de padrões suspeitos
13, 16	Implementar *firewalls,* **IDS,** limitação de taxa, balanceamento de carga e escalabilidade dinâmica
17	Adotar o princípio do menor privilégio, monitorizar com *logs* imutáveis e auditar ações no sistema.
21, 23	Aplicar uma autenticação robusta com **políticas de senha fortes** e, para complementar, **autenticação multifator**. Uso de **TLS** e **mTLS** para haver uma gestão adequada de chaves e reforçar a autenticação entre microsserviços com o uso de **OAuth**
26	Utilização de TLS forte para todas as comunicações, implementar mecanismos de integridade e monitorização de *patches* ou desabilitação da funcionalidade referente à vulnerabilidade com o intuito de prevenir quaisquer ataques
36, 37	Implementar controles de acesso rigorosos (**RBAC** e princípio do menor privilégio), isolar processos utilizando, por exemplo, ferramentas do próprio **Fedora 41** como o **SELinux** e, verificar *patches* para ver se o problema foi revisado para aquela versão
38, 39	Implementar **MFA,** usar **PBKDFs** com *salt* aleatório e armazenar senhas com módulos nativos (**Android Keystore/iOS Keychain**). Além disso, proteger atualizações com assinaturas digitais e realizar verificações periódicas de integridade
40	Utilizar assinaturas digitais para assegurar que apenas código legítimo seja executado, implementar verificação de integridade com *hashes* **SHA-256** para detetar alterações não autorizadas e aplicar ocultação do código com restrição de depuração para proteger contra engenharia reversa

Tabela 26: Tabela referente às mitigações - Parte 1

41	A aplicação verifica a assinatura digital dos ficheiros locais antes do uso; se for detetada qualquer alteração, o ficheiro é descartado para prevenir ataques e garantir a segurança dos dados
43,44	Os dados em repouso serão encriptados com **AES-256** e a comunicação protegida via **TLS 1.3**, garantindo confidencialidade e integridade. Políticas de acesso restritivas assegurarão que apenas utilizadores autenticados acedam a informações sensíveis
48	Implementação de autenticação mútua via **TLS 1.3** com certificados digitais e uso de **OAuth 2.0** para autenticação de utilizadores
51	Implementação de **logging seguro** e **assinatura digital** de transações para garantir a rastreabilidade das comunicações
47, 54	Implementação do princípio do **menor privilégio**, **autenticação multifator (MFA)** e **auditoria** rigorosa dos acessos ao sistema

Tabela 27: Tabela referente às mitigações - Parte 2

7. Conclusão

Este relatório apresentou uma análise detalhada dos requisitos de segurança do **Cofre Digital**, abordando as potenciais ameaças ao sistema e os mecanismos de mitigação necessários para garantir a **confidencialidade, integridade e disponibilidade** dos dados armazenados.

Quanto à nossa satisfação e opinião sobre o desempenho no trabalho ficamos satisfeitos com o resultado final mas achamos que há pontos a melhorar, especialmente em relação à organização das fraquezas e mitigações. Isto sendo que não tivemos em atenção que haviam pontos que poderiam ser agrupados, levando a que houvesse algum conteúdo repetido nas tabelas. O nosso objetivo final seria mapear todas as fraquezas e mitigações iguais e atribuir-lhes ID's únicos, porém, por motivo de falta de tempo acabamos por dar menos prioridade à organização das tabelas.