Tecnologias de Segurança

Análise de Segurança para o Serviço de Cofre Digital

Eduardo Cunha PG55939
João Magalhães PG55956
Rodrigo Gomes PG56004

Março, 2025

Indice

1. Introdução

Este trabalho tem como objetivo estudar e analisar a segurança do Cofre Digital, uma aplicação concebida para o armazenamento e partilha segura de ficheiros. Desenvolvido como uma solução fiável, o sistema assegura a confidencialidade e integridade dos dados, oferecendo ainda funcionalidades avançadas de partilha, tanto online como offline, através de uma aplicação móvel.

O foco principal desta investigação é garantir a segurança da aplicação antes da sua implementação. Para isso, são analisados os principais componentes do sistema, os ativos são identificados e categorizados, avaliadas as ameaças e os respetivos riscos. Com base nesta análise, são definidos requisitos de segurança e propostas soluções para mitigar os riscos identificados.

A metodologia adotada incluiu a modelação do sistema, a identificação de ameaças, a análise de riscos e a validação do modelo. Este processo foi conduzido de forma iterativa, assegurando que nenhum aspeto relevante fosse negligenciado. Para a identificação de ameaças, recorreram-se a modelos como o STRIDE e a referências como o OWASP Top 10, complementadas com sessões de *brainstorming*, garantindo uma abordagem abrangente.

2. Descrição do Cofre Digital

O sistema é composto por três componentes principais:

- **Servidor:** Responsável pela lógica do serviço, incluindo registo e autenticação de utilizadores, controlo de acesso, gestão de cofres, grupos, pastas e armazenamento de ficheiros. Opera através de microsserviços em cloud, utilizando tecnologias como Fedora Server 41, Nginx 1.24.0 e PostgreSQL 10.22.
- **Serviço Web:** Permite o registo, gestão de cofres, ficheiros, pastas, grupos e permissões de partilha.
- **Aplicação Móvel:** Suporta todas as funcionalidades do serviço web e inclui modo offline com cópia local do cofre. Permite transferência segura de ficheiros via Bluetooth entre dispositivos, sem intervenção do servidor. Desenvolvida como uma *Progressive Web App* (PWA).

2.1. Funcionalidades de Partilha

O sistema suporta:
- Partilha de ficheiros ou pastas com utilizadores ou grupos.
- Criação de grupos (ex.: “família”, “trabalho”) por qualquer utilizador, mediante a identificação dos membros.
- Definição de permissões de partilha, onde o proprietário pode autorizar ou não a redistribuição do conteúdo por parte dos destinatários.

2.2. Requisitos globais

O sistema deve garantir:
- **Confidencialidade:** Proteção contra acessos não autorizados.

- **Integridade:** Prevenção de alterações não autorizadas ou acidentais dos dados.
- **Autenticidade:** Processo robusto de autenticação para garantir que apenas utilizadores autorizados acedem ao cofre.

Estes requisitos asseguram um ambiente seguro e fiável para os utilizadores.

2.3. Representação do Sistema

Seguem-se os modelos (alto nível) da arquitetura percecionada inicialmente para o Cofre Digital, bem como a arquitetura final que definimos, com o objetivo de reduzir a complexidade em termos de segurança.

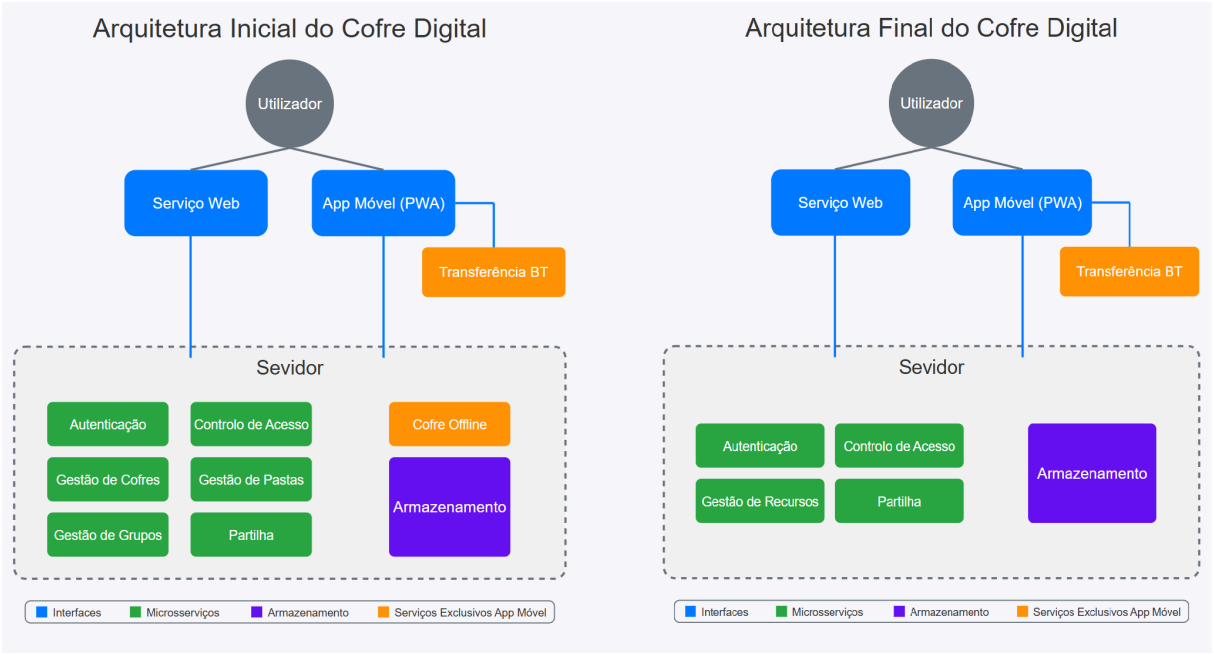

Figure 1: Arquitetura Percecionada *vs* Arquitetura Final do Cofre Digital

2.3.1. Perceção Inicial

A arquitetura do Cofre Digital baseia-se em microsserviços, garantindo modularidade, escalabilidade e manutenção eficiente. Esta abordagem permite desenvolver, atualizar e escalar componentes isoladamente, melhorando a resiliência e a distribuição da carga na cloud. A flexibilidade do sistema suporta múltiplas interfaces, como web e móvel, assegurando uma experiência contínua e unificada entre as plataformas. A aplicação móvel, desenvolvida como PWA, permite cópias locais dos cofres e transferências Bluetooth, aumentando a acessibilidade, mas trazendo desafios adicionais.

Tais desafios baseiam se sobretudo no que diz respeito à segurança. A existência dos serviços e consequente inter-comunicação expande a superfície de ataque, exigindo autenticação, encriptação e monitorização rigorosas.

2.3.2. Arquitetura Final

Na arquitetura percecionada inicialmente, o servidor era composto por vários microsserviços bem segmentados. Existiam serviços distintos para gestão de cofres, grupos e pastas, autenticação, controlo de acesso e partilha. Além disso, havia um serviço de armazenamento e um exclusivo para a gestão de cofres offline, acessível através da aplicação móvel. Esta abordagem

proporcionava uma separação clara de responsabilidades, mas também aumentava a complexidade do sistema e a superfície de ataque que poderia vir a ser explorada.

Na versão modificada da arquitetura, alguns serviços foram agregados. A gestão de cofres (inc. *offline*), grupos e pastas foi unificada num único serviço, pelo simples facto de que a noção de cofre agrupa nada mais que pastas, ficheiros e grupos, reduzindo a necessidade de comunicação entre múltiplos microsserviços e, consequentemente, diminuindo a superfície de ataque. No entanto, não se optou por uma fusão completa de todos os serviços, em caso extremo de redução de superfície, pois isso centralizaria demasiadas responsabilidades num único ponto, o que poderia comprometer não só a escalabilidade e manutenção do sistema (pontos importantes, embora não relacionados diretamente com a segurança), mas também permitir que um atacante com acesso ao serviço pudesse controlar todo o sistema. A equipa de desenvolvimento encontrou um meio-termo onde a segurança foi reforçada sem comprometer inteiramente a modularidade.

Apesar destas mudanças, alguns serviços mantiveram-se inalterados. O serviço de autenticação continuou separado, sendo que lida com dados sensíveis e deve estar isolado para reduzir o risco de comprometimento. O controlo de acesso também se manteve independente da gestão de recursos, garantindo que um atacante com acesso aos recursos não pudesse automaticamente modificar permissões ou escalar privilégios, e vice-versa. O serviço de armazenamento permaneceu como uma entidade distinta, pois é um componente crítico cuja estabilidade e desempenho são essenciais para o funcionamento do sistema.

A principal vantagem da nova abordagem foi a redução da complexidade e da superfície de ataque. No entanto, cada decisão representou um compromisso. A agregação de serviços reduziu a necessidade de comunicações internas e possíveis vulnerabilidades, mas aumentou a responsabilidade de alguns serviços. No final, a equipa encontrou um equilíbrio entre segurança e desempenho, garantindo que o sistema seja mais seguro, sem se tornar excessivamente complexo (ou centralizado) ou difícil de escalar.

2.3.3. Outras abordagens arquiteturais

Qualquer decisão arquitetural não passa de um *trade-off* entre duas ou mais características. Dito isto, para além da arquitetura com que o grupo decidiu avançar, é também de elevada importância mencionar outras soluções idealizadas, e mais que isso concluir sobre as vantagens e desvantagens de ter seguido com essa nova arquitetura.

As alterações mais relevantes incidiriam no modelo de armazenamento, pelo que vamos direcionar maioritariamente o foco para esse aspeto. A escolha entre o modelo integrado (base de dados única) e o modelo híbrido agora apresentado, que envolve a utilização não só de uma base de dados, mas também de um servidor de ficheiros, envolve compromissos importantes que afetam segurança, desempenho, custo e complexidade operacional.

Ao armazenar tudo numa base de dados, elimina-se o risco de inconsistências entre ficheiros e metadados, pois todas as operações ocorrem em transações atómicas. A gestão operacional é simplificada com apenas um sistema para manter. Esta abordagem também proporciona um modelo de segurança com controlo de acesso unificado e superfície de ataque reduzida. Contudo, sacrifica desempenho e escalabilidade. As bases de dados não são otimizadas para

armazenar e recuperar grandes volumes de dados binários, resultando em operações mais lentas para ficheiros maiores. Do ponto de vista de segurança, representa um cenário de elevada responsabilidade com todos os recursos centrados num serviço que, se comprometido, todo o conteúdo pode ser exposto.

Por outro lado, o modelo híbrido oferece melhor desempenho e escalabilidade (bem como um modelo de base de dados fragmentada), com o custo de possuir maior complexidade. Ao armazenar os ficheiros num servidor dedicado, consegue-se otimização de performance, especialmente para ficheiros grandes. Os servidores de ficheiros são projetados especificamente para esta função (MinIO em Amazon S3, por exemplo). Esta abordagem também permite implementar cifragem individual dos ficheiros. O preço desta flexibilidade é a complexidade acrescida. O modelo híbrido requer mecanismos adicionais para manter a consistência entre sistemas, aumenta a potencial superfície de ataque e introduz desafios na gestão das chaves criptográficas de cada ficheiro. O principal *trade-off* é, portanto, entre simplicidade operacional e consistência garantida (modelo integrado) *versus* melhor desempenho, escalabilidade e segurança em camadas (modelo híbrido).

2.3.4. Diagrama de Fluxo de Dados

Para complementar a definição da arquitetura, elaborámos um Diagrama de Fluxo de Dados (DFD) que representa, de forma clara e estruturada, a circulação de informações no sistema. Este diagrama simplifica a visualização das interações entre os diferentes componentes durante operações como gestão de cofres, pastas, ficheiros, grupos, autenticação e controlo de acessos.

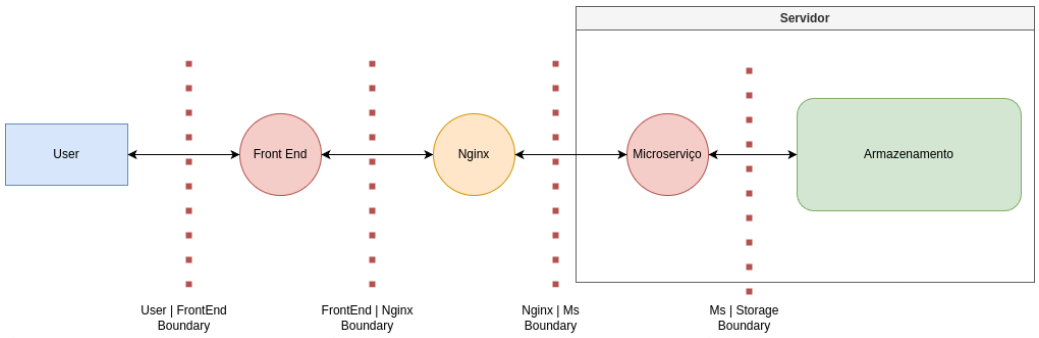

Figure 2: Diagrama de Fluxo de dados

A criação deste diagrama ajudou-nos a consolidar a visão do sistema, destacando pontos críticos onde a segurança deve ser reforçada.

3. Gestão de Ativos

Fizemos uma distinção lógica em relação aos ativos, classificando-os dentro das categorias *standard* como *Restricted*, *Confidential*, *Internal-only* e *Public*. Os ativos *Restricted* constituem ativos extremamente sensíveis, cuja exposição pode comprometer a segurança do sistema e dos seus utilizadores. Os ativos *Confidential* são fundamentais para o funcionamento do sistema, pelo que devem ser mantidos com alto controlo de acesso. Os ativos *Internal-only* são informações internas da empresa, mas sem natureza crítica para segurança, enquanto os ativos *Public* são acessíveis ao público geral e não apresentam impactos em caso de comprometimento.

3.1. Identificação de Ativos

3.1.1. *Restricted*

- **Dados dos Utilizadores:** Inclui credenciais de autenticação (hashes, tokens), informações pessoais associadas à conta.
- **Cofres Digitais:** Conjunto de ficheiros e pastas armazenados pelos utilizadores, organizados em cofres. Inclui tanto os metadados (nomes, permissões, datas) como os próprios conteúdos cifrados. Neste ativo, está incluída uma cópia do cofre para permitir a partilha offline.
- **Chaves de Encriptação:** Chaves utilizadas para cifrar os ficheiros nos cofres, proteger comunicações e autenticar utilizadores.
- **Permissões de Acesso e Partilha:** Regras que definem quem pode aceder, modificar ou partilhar ficheiros e pastas. Inclui permissões individuais e de grupo.
- **Registos de Atividade:** Histórico detalhado de ações realizadas pelos utilizadores e pelo sistema. Pode incluir tentativas de login, acessos a ficheiros e mudanças de permissões.
- **Serviço de Autenticação:** Microsserviço dedicado à gestão da identidade dos utilizadores, incluindo login, logout, verificação de tokens e MFA.
- **Base de Dados (PostgreSQL 10.22):** Contém informações sobre utilizadores, cofres, permissões, metadados e ficheiros armazenados.

3.1.2. *Confidential*

- **Sistema Operativo (Fedora Server 41):** Hospeda os serviços backend na infraestrutura cloud.
- **Código da Aplicação:** Código-fonte da aplicação web e móvel, incluindo microsserviços do backend.
- **Servidor Web (Nginx 1.24.0):** Responsável por gerir as comunicações entre utilizadores e o backend, fazendo proxy de pedidos HTTP(s).
- **Comunicação Bluetooth:** Permite transferência de ficheiros diretamente entre dispositivos sem passar pelo servidor.

3.1.3. *Internal-only*

- **Grupos de Utilizadores:** Estruturas para organizar os utilizadores em grupos, facilitando a partilha de ficheiros.
- **Aplicação Móvel (Código Distribuído):** Versão distribuída da aplicação móvel (binários).
- **Configuração da Infraestrutura Cloud:** Detalhes sobre a configuração dos servidores e serviços utilizados.

3.1.4. *Public*

- **Documentação Pública:** Guias de utilização e documentação técnica divulgada publicamente.

- **Identidade Visual da Aplicação:** Logótipos, temas e elementos gráficos usados na interface.
- **Informações Gerais sobre Arquitetura:** Diagramas e explicações de alto nível sobre o funcionamento do sistema.

4. Principais Ameaças

As principais ameaças identificadas estão alinhadas com as vulnerabilidades mais comuns do ***OWASP Top 10*** e do ***CWE***. Para a análise de vulnerabilidades, foi utilizada a metodologia STRIDE como base.

4.1. Ativos *Restricted*

Dados dos Utilizadores:

- Roubo de credenciais através de phishing ou ataques de força bruta (**Spoofing**).
- Exposição de informação sensível devido a vulnerabilidades de autenticação (**Information Disclosure**).
- Uso de credenciais comprometidas para escalar privilégios no sistema (**Elevation of Privilege**).

Vulnerabilidades: Autenticação insuficiente (OWASP A07:2021), armazenamento inseguro de credenciais (OWASP A02:2021).

Cofres Digitais:

- Quebra de integridade dos cofres por modificações indevidas (**Tampering**).
- Perda de confidencialidade devido a acesso não autorizado (**Information Disclosure**).
- Risco de ransomware ou corrupção de dados (**Denial of Service**).

Vulnerabilidades: Falhas de validação de entrada (OWASP A03:2021), falhas de controlo de acesso (OWASP A01:2021), encriptação inadequada (OWASP A02:2021)).

Chaves de Encriptação:

- Roubo de chaves devido a armazenamento inseguro (**Information Disclosure**).
- Perda de confidencialidade devido a acesso não autorizado (**Information Disclosure**).

Vulnerabilidades: Encriptação inadequada (OWASP A02:2021), gestão insegura de secrets (OWASP A07:2021).

Permissões de Acesso e Partilha:

- Configurações inadequadas podem permitir a ampliação indevida de acessos (**Elevation of Privilege**).
- Omissão de registos de alterações pode resultar em dificuldades para rastrear responsáveis (**Repudiation**).

Vulnerabilidades: Falhas de controlo de acesso (OWASP A01:2021), falhas de configuração (OWASP A05:2021).

Registos de Atividade:

- Manipulação de logs para ocultar atividades maliciosas (**Tampering**).
- Exposição indevida de informações sensíveis nos logs (**Information Disclosure**).

Vulnerabilidades: Falhas de controlo de acesso (OWASP A01:2021), falhas de auditoria (OWASP A09:2021).

Serviço de Autenticação:

- Comprometimento do serviço levando à autenticação indevida (**Spoofing**).
- Bypass de verificações de MFA (**Elevation of Privilege**).
- Ataques de negação de serviço ao sistema de autenticação (**Denial of Service**).

Vulnerabilidades: Falhas de implementação de autenticação (OWASP A07:2021), vulnerabilidades em sessões (OWASP A01:2021).

Base de Dados (PostgreSQL 10.22):

- Injeção de SQL para acesso indevido a dados sensíveis (**Tampering**).
- Perda de integridade dos dados devido a ataques maliciosos ou corrupção acidental (**Elevation of Privilege**/**Tampering**).

Vulnerabilidades: Injeção SQL (OWASP A03:2021), configurações incorretas de segurança (OWASP A05:2021).

4.2. Ativos *Confidential*

Sistema Operativo (Fedora Server 41):

- Escalação de privilégios através de exploração de vulnerabilidades do kernel (**Elevation of Privilege**).
- Comprometimento do sistema devido a pacotes desatualizados ou não corrigidos (**Tampering**).

Vulnerabilidades: Uso de componentes desatualizados (OWASP A06:2021), falhas de configuração (OWASP A05:2021) e Falhas na integridade de software e dados (OWASP A08:2021).

Código da Aplicação:

- Presença de vulnerabilidades de segurança devido a falhas de desenvolvimento (**Tampering**).
- Injeção de código malicioso por terceiros (**Elevation of Privilege**/**Tampering**).
- Ataque MITM devido a falta de segurança de canais de comunicação entre cliente/servidor e serviços. (**Tampering**/**Information Disclosure**)
- Comprometimento de Service Workers da aplicação PWA devido a erros de configuração.

Vulnerabilidades: Injeção de código (OWASP A03:2021), uso de componentes vulneráveis (OWASP A06:2021).

Servidor Web (Nginx 1.24.0):

- Ataques de negação de serviço para interromper o acesso ao sistema (**Denial of Service**).
- Configurações incorretas podem permitir ataques de cross-site scripting (XSS) (**Information Disclosure**).

Vulnerabilidades: Configurações incorretas de segurança (OWASP A05:2021), falhas de validação de entrada (OWASP A03:2021).

Comunicação Bluetooth:

- Ataques de man-in-the-middle durante a transmissão de ficheiros (**Tampering**/**Information Disclosure**).

Devido à natureza heterogénea dos dispositivos que utilizarão a comunição Bluetooth, bem como as respetivas versões do protocolo a correr em cada um deles, e sendo que não se pretende implementar qualquer tipo de requisitos mínimos de utilização, partiremos do princípio que a segurança do canal de comunicação nunca é assegurada. Assim sendo, irá ser retirada qualquer responsabilidade à camada de comunicação, deixando as garantias de autenticidade, confidencialidade e integridade a cargo da camada aplicacional.

Vulnerabilidades: Encriptação inadequada (OWASP A02:2021), falhas de autenticação (OWASP A07:2021).

4.3. Ativos *Internal-Only*

Grupos de Utilizadores:

- Acessos indevidos por utilizadores mal intencionados (**Spoofing**).
- Permissões incorretas podem levar a divulgação de dados privados (**Information Disclosure**).

Vulnerabilidades: Falhas de controlo de acesso (OWASP A01:2021), configurações incorretas de segurança (OWASP A05:2021).

Aplicação Móvel (Código Distribuído):

- Exploração de vulnerabilidades do código da aplicação (**Tampering**).
- Roubo de dados locais devido a dispositivos comprometidos (**Information Disclosure**).

Vulnerabilidades: Falhas de validação de entrada (OWASP A03:2021), encriptação inadequada (OWASP A02:2021).

Configuração da Infraestrutura Cloud:

- Ameaças de ataques distribuídos de negação de serviço (DDoS) comprometendo a disponibilidade (**Denial of Service**).
- Acesso não autorizado à infraestrutura (**Spoofing/Elevation of Privilege**).

Vulnerabilidades: Falhas de configuração de rede (OWASP A05:2021), falta de proteção contra DoS (OWASP A08:2021).

4.4. Ativos *Public*

Documentação Pública:

- Exposição de informações que podem facilitar ataques (**Information Disclosure**).
- Documentação desatualizada pode levar a más práticas pelos utilizadores (**Tampering** indiretamente).

Vulnerabilidades: Exposição excessiva de informações (OWASP A01:2021) e documentação desatualizada (OWASP A06:2021) .

Identidade Visual da Aplicação:

- Imitação da interface para ataques de phishing (**Spoofing**).
- Uso indevido da marca para criar aplicações falsas (**Repudiation**).

Vulnerabilidades: Não tem vulnerabilidades associadas diretamente.

Informações Gerais sobre Arquitetura:

- Exposição de detalhes que facilitam a identificação de vetores de ataque (**Information Disclosure**).

Vulnerabilidades: Exposição excessiva de informações do sistema (OWASP A05:2021).

5. Análise de Risco

A análise de risco é uma etapa crucial para garantir a segurança do sistema Cofre Digital. Com base nas ameaças identificadas anteriormente, é necessário avaliar o impacto e a probabilidade de ocorrência de cada uma delas, permitindo priorizar as ações de mitigação. A metodologia utilizada segue os seguintes passos:

1. **Identificação das Ameaças:** Já realizada no capítulo anterior, com base na metodologia *STRIDE* e no *OWASP Top 10*.
2. **Avaliação do Impacto:** Classificação do impacto (Baixo, Médio ou Alto) dependendo da gravidade das consequências para o sistema e para os utilizadores.
3. **Avaliação da Probabilidade:** Classificação da probabilidade (Baixa, Média ou Alta) com base na facilidade de exploração da vulnerabilidade e na exposição do sistema.
4. **Cálculo do Risco:** O risco é calculado com base na combinação do impacto e da probabilidade. Segue a categorização de risco que nós consideramos:

Impacto/Probabilidade	Baixa	Média	Alta
Baixo	Risco Negligível	Risco Baixo	Risco Moderado
Médio	Risco Baixo	Risco Moderado	Risco Alto
Alto	Risco Moderado	Risco Alto	Risco Crítico

5.1. Avaliação de Risco por Categoria de Ativos

A avaliação baseia-se na medição do impacto e da probabilidade, com as categorias definidas da seguinte forma:

Avaliação do Impacto:

- **Baixo:** Efeitos mínimos, afeta poucos utilizadores ou partes do sistema, sem impacto legal ou financeiro significativo.
- **Médio:** Impacto moderado, afeta utilizadores ou processos importantes, com possíveis custos ou penalizações.

- **Alto:** Impacto grave, afeta todo o sistema, com perda de dados ou danos significativos, implicações legais ou financeiras severas.

Avaliação da Probabilidade:

- **Baixa:** Requer condições raras ou conhecimento especializado, com exposição limitada.
- **Média:** Exposição moderada, ataques possíveis com recursos medianos e histórico de incidentes.
- **Alta:** Vulnerabilidade fácil de explorar, com alta exposição e histórico frequente de ataques.

Com esta sistematização da avaliação de impacto, probabilidade e, por consequência, do risco, consideramos ter definido uma metodologia consistente para a análise sucessiva de riscos.

5.1.1. Ativos Restricted

Os ativos classificados como Restricted são os mais sensíveis do sistema, e qualquer comprometimento pode ter consequências graves.

Ameaça	Impacto	Probabilidade	Risco
Roubo de credenciais (Spoofing)	Alto	Alta	Crítico
Exposição de dados (Information Disclosure)	Alto	Média	Alto
Uso de credenciais comprometidas (Elevation of Privilege)	Alto	Média	Alto
Quebra de integridade dos cofres (Tampering)	Alto	Média	Alto
Perda de confidencialidade por acesso não autorizado (Information Disclosure)	Alto	Média	Alto
Ransomware ou corrupção de dados (Denial of Service)	Alto	Média	Alto
Roubo de chaves de encriptação (Information Disclosure)	Alto	Baixa	Moderado
Configurações inadequadas de permissões (Elevation of Privilege)	Médio	Alta	Alto
Omissão de registos de alterações (Repudiation)	Médio	Baixa	Baixo
Manipulação de logs (Tampering)	Médio	Baixa	Baixo
Comprometimento do serviço de autenticação (Spoofing/DoS)	Alto	Média	Alto
Negação de serviço ao sistema de autenticação (Denial of Service)	Alto	Média	Alto
Contornar a autenticação multifator MFA (Elevation of Privilege)	Alto	Média	Alto
Injeção SQL (Elevation of Privilege)	Alto	Média	Alto
Perda de integridade dos dados por ataques maliciosos (Tampering)	Alto	Média	Alto

5.1.2. Ativos Confidential

Os ativos Confidential são essenciais para o funcionamento do sistema, mas o seu comprometimento não é tão crítico quanto os ativos Restricted.

Ameaça	Impacto	Probabilidade	Risco
Elevação de privilégios no SO (Elevation of Privilege)	Alto	Baixa	Moderado
Comprometimento do sistema por pacotes desatualizados (Tampering)	Alto	Média	Alto
Vulnerabilidades no código da aplicação (Tampering)	Médio	Média	Moderado
Injeção de código malicioso (Elevation of Privilege)	Médio	Média	Moderado
Ataques de negação de serviço (DoS)	Médio	Alta	Alto
Configurações incorretas no Nginx (Information Disclosure)	Médio	Média	Moderado
Interceção de comunicações Bluetooth (Information Disclosure)	Médio	Média	Moderado

5.1.3. Ativos Internal-Only

Os ativos Internal-Only são menos críticos, mas o seu comprometimento pode afetar a operação interna do sistema.

Ameaça	Impacto	Probabilidade	Risco
Acessos indevidos a grupos (Spoofing)	Médio	Média	Moderado
Divulgação de dados privados (Information Disclosure)	Médio	Média	Moderado
Exploração de vulnerabilidades na app móvel (Tampering)	Médio	Baixa	Baixo
Roubo de dados locais (Information Disclosure)	Médio	Baixa	Baixo
Ataques DDoS à infraestrutura (Denial of Service)	Alto	Média	Alto
Acesso não autorizado à infraestrutura (Spoofing/Elevation of Privilege)	Alto	Média	Alto

5.1.4. Ativos Public

Os ativos Public são de baixa criticidade, mas o seu comprometimento pode afetar a reputação da empresa.

Ameaça	Impacto	Probabilidade	Risco
Exposição de informações na documentação (Information Disclosure)	Baixo	Alta	Baixo
Documentação desatualizada (Tampering)	Baixo	Média	Baixo
Imitação da interface para phishing (Spoofing)	Médio	Média	Moderado
Uso indevido da marca (Repudiation)	Médio	Baixa	Baixo
Exposição de detalhes e utilização de informações arquiteturais (Information Disclosure)	Baixo	Média	Baixo

6. Requisitos de Segurança e Sugestões de Resposta

Nesta secção, são apresentados os requisitos de segurança e sugestões de resposta para mitigar as ameaças identificadas nos capítulos anteriores. Estas recomendações visam garantir a confidencialidade, integridade e disponibilidade dos ativos do sistema Cofre Digital.

6.1. Requisitos de Segurança para Ativos Restricted

1. **Autenticação Robusta:** Implementar MFA (Multi-Factor Authentication) utilizando OAuth 2.0 ou OpenID Connect.
   Sugestão: Exigir MFA para todos os acessos sensíveis, incluindo contas administrativas, e utilizar autenticação baseada em chaves.
2. **Proteção Contra Ataques:** Implementar deteção de login suspeito e bloqueios após tentativas falhadas.
   Sugestão: Implementar CAPTCHA e monitorizar tentativas de acesso suspeitas.
3. **Encriptação de Ficheiros:** Utilizar AES-256 para dados em repouso e TLS 1.3 para transmissão.
   Sugestão: Utilizar bibliotecas de criptografia amplamente testadas, como OpenSSL ou BouncyCastle.
4. **Controlo de Acesso Granular:** Implementar RBAC (Role-Based Access Control) e revisões periódicas de permissões.
   Sugestão: Automatizar a revogação de permissões não utilizadas.
5. **Armazenamento Seguro de Chaves:** Utilizar HSMs (Hardware Security Modules) ou serviços de gestão de chaves.
   Sugestão: Implementar rotação automática de chaves.
6. **Tokens JWT com Expiração Curta:** Utilizar tokens JWT com um tempo de expiração curto para reduzir o risco de reutilização de tokens comprometidos.
7. **Registo de Alterações:** Garantir logging centralizado com ferramentas como ELK Stack.
   Sugestão: Implementar alertas em tempo real para alterações críticas.
8. **Menor Privilégio:** Aplicar o princípio do menor privilégio para acesso controlado.
   Sugestão: Realizar revisões periódicas das permissões atribuídas.
9. **Proteção Contra Manipulação de Logs:** Utilizar assinaturas digitais e armazenamento imutável.
   Sugestão: Armazenar logs externamente com trilha de auditoria.
10. **Uniformizar mensagens de erro:** Evitar exposição de mensagens de erro detalhadas.
11. **Gestão de Informações Sensíveis:** Implementar máscara de dados sensíveis nos logs.
12. **Mitigação de Ataques DoS:** Implementar rate limiting e WAF (Web Application Firewall).
    Sugestão: Utilizar serviços de mitigação de DDoS em cloud, como Cloudflare ou AWS Shield.

13. **Proteção Contra Injeção SQL:** Implementar filtros de entrada rigorosos e validar todos os inputs.
14. **Backups Seguros:** Implementar backups encriptados com testes regulares de recuperação, garantindo a integridade dos dados. Dada a centralização da base de dados, este processo torna-se ainda mais crítico.

6.2. Requisitos de Segurança para Ativos Confidential

15. **Atualizações Frequentes:** Implementar patches automáticos.
16. **Acesso Restrito:** Usar SSH com autenticação por chave e desativação do login root.
17. **Análise de Segurança:** Utilizar ferramentas de análise estática, como SonarQube.
18. **Validação de Entrada:** Aplicar técnicas de sanitização contra injeções de código (XSS).
19. **Comunicação Segura:** Garantir comunicação entre servidor/cliente sobre HTTPS/TLS e entre serviços com dupla autenticação.
20. **Service Workers (PWA):** Garantir registo de Service Workers apenas a partir de fontes confiáveis.
21. **Segurança na Comunicação:** Ativar TLS 1.2/1.3 e cabeçalhos de segurança (ex.: Strict-Transport-Security, Content-Security-Policy).
22. **Encriptação Bluetooth:** Aplicar AES-CCM (Counter com CBC-MAC) na comunicação Bluetooth.
    Sugestão: Utilizar certificados digitais para autenticação mútua.

6.3. Requisitos de Segurança para Ativos Internal-Only

23. **Gestão Segura de Grupos:** Aprovações manuais para criação de grupos.
    Sugestão: Implementar revisões periódicas de membros e permissões.
24. **Proteção de Dados:** Aplicar máscaras de dados sensíveis em interfaces.
25. **Segurança Local:** Os dados armazenados localmente serão protegidos por criptografia, garantindo que apenas utilizadores autorizados possam acessá-los.
    Sugestão Usar Keychain (iOS) e Keystore (Android) para armazenamento seguro de chaves e credenciais, criptografia do banco de dados local (ex.: SQLCipher para SQLite), além de técnicas como detecção de Root (Android) e Jailbreak (iOS) para reforçar a segurança contra acessos não autorizados.
26. **Controlo de Acesso:** Aplicação de IAM (Identity and Access Management) restritivo.

6.4. Requisitos de Segurança para Ativos Public

27. **Proteção Contra Exposição:** Revisões frequentes para evitar exfiltração de informações.
    Sugestão: Utilizar ferramentas de deteção de exfiltrações.
28. **Atualizações Regulares:** Manter a documentação precisa e atualizada.
29. **Prevenção de Phishing:** Monitorizar lojas de apps para evitar clones maliciosos.

30. **Consciencialização:** Informar utilizadores sobre ataques de phishing.

31. **Restrições de Divulgação:** Evitar exposição de detalhes críticos.

6.5. Requisitos Gerais de Segurança

- **Monitorização Contínua:** A monitorização contínua é essencial para garantir a deteção precoce de atividades maliciosas ou anomalias no sistema. A implementação de uma solução de SIEM (Security Information and Event Management), como Splunk, permite agregar e analisar logs de diferentes componentes do sistema, facilitando assim a identificação de atividades suspeitas.
- **Resposta a Incidentes:** Ter um plano de resposta a incidentes bem definido é crucial para minimizar o impacto de eventuais violações de segurança. Este plano deve incluir procedimentos claros para a contenção, erradicação e recuperação de incidentes, bem como a comunicação com as partes afetadas.
- **Testes de Segurança:** A realização de testes de segurança regulares é fundamental para identificar e corrigir vulnerabilidades antes que sejam exploradas por atacantes. Estes testes devem seguir metodologias reconhecidas, como o OWASP Testing Guide e o PTES (Penetration Testing Execution Standard), para garantir uma cobertura abrangente.

6.6. Boas Práticas de Segurança: PostgreSQL, Nginx e Fedora

Relativamente à utilização do PostgreSQL, Nginx e Fedora, neste capítulo vamos verificar se existem requisitos de segurança adicionais, tendo em conta as versões especificadas pela empresa que irá prestar o serviço. Vamos analisar cada um dos componentes.

A versão 10.22 do PostgreSQL já atingiu o fim do seu ciclo de vida, o que significa que não recebe mais atualizações de segurança e está sujeita a eventuais vulnerabilidades que possam ter sido descobertas e corrigidas em versões posteriores. A melhor abordagem seria atualizar para versões mais recentes. No entanto, considerando que a empresa pretende utilizar esta versão, é essencial adotar alguns cuidados redobrados, tais como:

- Configurar backups regulares e testar os procedimentos de recuperação.
- Desativar funcionalidades não utilizadas para reduzir a superfície de ataque.

No caso do Nginx 1.24.0, esta é uma versão relativamente recente e, até à data, não existem vulnerabilidades conhecidas associadas a esta versão. Assim, não implicam requisitos específicos adicionais, uma vez que já foram definidos requisitos de segurança para o sistema de rede.

O mesmo se aplica ao Fedora 41, que é uma versão atualizada com suporte regular. Até à data, não existem vulnerabilidades conhecidas associadas a esta versão, pelo que não necessita de requisitos extra além daqueles que já foram definidos para o sistema operativo.

6.7. Segurança na Cloud

Independentemente da natureza do *Cloud Provider* utilizado (IaaS ou PaaS), a segurança na cloud deve ir para além das garantias do *provider*, dado que a proteção dos dados continua a ser responsabilidade da organização.

Assim, embora o hardware do provider não seja exatamente considerado um ativo, os dados armazenados e transmitidos devem ser protegidos contra potenciais ameaças, incluíndo ataques ao hardware. Entre os ataques mais comuns ao hardware, destacam-se os de canal lateral, falhas na virtualização e acessos físicos não autorizados. A solução da organização para mitigação desses riscos passa pela adoção de encriptação forte, ponto-a-ponto, comunicação segura e mecanismos de autenticação robustos. A encriptação ponto-a-ponto a ser implementada garante que a informação é cifrada antes do envio e apenas decifrada pelo utilizador autorizado. Dessa forma, mesmo que a infraestrutura do provider seja comprometida, os dados permanecem inacessíveis sem as chaves correspondentes, culminando numa (desejada) independência do *cloud provider*.

7. Conclusão

Neste trabalho, realizamos um estudo aprofundado da aplicação Cofre Digital, com foco na sua segurança. Após o levantamento dos ativos, análise de ameaças e avaliação de riscos, definimos requisitos de segurança e propusemos soluções que considerámos eficazes para mitigar as vulnerabilidades identificadas. Incluímos também melhorias na arquitetura do sistema, que representaram *trade-offs* equilibrados entre segurança, funcionalidade e simplicidade. Estas alterações permitiram reduzir a superfície de ataque e simplificar a infraestrutura, sem comprometer a usabilidade do sistema.

Consideramos que alcançámos todos os objetivos definidos inicialmente, embora o número limitado de páginas tenha sido uma barreira para a profundidade que pretendíamos alcançar no nosso trabalho. Ainda assim, sentimos que conseguimos estruturar de forma sólida as nossas soluções e apresentar uma especificação segura para o Cofre Digital.

Esta análise foi fundamental para a solidificação e o aprofundamento dos nossos conhecimentos na área da cibersegurança. Além de nos ter permitido desenvolver várias competências em segurança da informação, também nos proporcionou o desenvolvimento de capacidades na área da investigação, habilidades essas que consideramos essenciais no domínio da área.

8. Bibliografia

- OWASP Foundation. (2021). OWASP Top Ten Web Application Security Risks. Disponível em: https://owasp.org/www-project-top-ten/°.
- Microsoft. (2023). STRIDE Threat Model. Disponível em: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-stride°.
- NIST. (2020). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations.
- PostgreSQL Global Development Group. (2022). PostgreSQL 10.22 Documentation. Disponível em: https://www.postgresql.org/docs/10/index.html°.
- Nginx, Inc. (2023). Nginx Documentation. Disponível em: https://nginx.org/en/docs/°.
- Fedora Project. (2024). Fedora 41 Security Guide. Disponível em: https://docs.fedoraproject.org/°.
- MITRE Corporation. (2023). Common Weakness Enumeration (CWE). Disponível em: https://cwe.mitre.org/°.
- Cloud Security Alliance (CSA). (2023). Security Guidance for Critical Areas of Focus in Cloud Computing.