UNIVERSIDADE NOVE DE JULHO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

PROJETO EM GESTAO DE SISTEMAS COMPUTACIONAIS

APLICAÇÃO WEB PARA COMPARTILHAMENTO SEGURO DE ARQUIVOS COM ARMAZENAMENTO TEMPORÁRIO EM NUVEM: UMA SOLUÇÃO PARA GESTÃO DE PROJETOS DE TI

Autores:
Vitória Akemi Corrêa Arakaki

São Paulo,

Novembro 2025

Documentação técnica - Desenvolvimento software “API Cloud”

Vitória Akemi Corrêa Arakaki RA: 422101990

Trabalho apresentado ao curso de Ciência da Computação da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau de Bacharelado em Ciência da Computação.

FOLHA DE APROVAÇÃO

Vitória Akemi Corrêa Arakaki RA: 422101990

PROJETO EM GESTAO DE SISTEMAS COMPUTACIONAIS

Trabalho acadêmico apresentado à disciplina de Projeto em Gestão de Sistemas Computacionais, sob orientação da Prof.ª Débora Virgília Canne, como requisito parcial para avaliação na Universidade Nove de Julho.

São Paulo, 15 de novembro de 2025

_____

Profa. Debora Virgilia Canne

AGRADECIMENTOS

A todos aqueles que contribuíram, de alguma forma, para a realização deste trabalho. A professora Debora Virgilia Canne, por ter sido minha orientadora e ter desempenhado tal função com dedicação e amizade, pela ajuda e pela paciência com a qual guiaram o nosso aprendizado.

- "A tecnologia é apenas uma ferramenta. No que diz respeito a motivar os alunos e fazer com que trabalhem juntos, o professor é o mais importante." - Bill Gates

RESUMO

Este trabalho tem como foco o desenvolvimento de uma aplicação web voltada para o gerenciamento seguro de arquivos. Especificamente, trata-se de um software capaz de realizar o envio e o recebimento de documentos digitais, utilizando armazenamento temporário em ambiente de nuvem.

A principal funcionalidade da aplicação consiste em garantir que os arquivos armazenados sejam automaticamente excluídos do banco de dados após serem acessados e clonados pelo destinatário. Esse processo visa aumentar a segurança da informação, evitando retenções indevidas e permitindo que os dados possam ser restaurados a partir de cópias autorizadas, quando necessário.

Além disso, o sistema foi projetado para operar com protocolos que asseguram a integridade dos arquivos durante a transferência, bem como mecanismos de rastreamento e controle de acesso, contribuindo para uma gestão eficiente e confiável dos dados compartilhados.

Palavras-Chaves: Desenvolvimento, Software, Segurança, Protocolos.

ABSTRACT

This work focuses on the development of a web application aimed at secure file management. Specifically, it is software capable of sending and receiving digital documents using temporary cloud storage.

The main functionality of the application is to ensure that stored files are automatically deleted from the database after being accessed and cloned by the recipient. This process aims to enhance information security by preventing unauthorized retention and allowing data to be restored from authorized copies when necessary.

Additionally, the system is designed to operate with protocols that ensure the integrity of files during transfer, as well as tracking and access control mechanisms, contributing to efficient and reliable management of shared data.

Keywords: Development, Software, Security, Protocols.

Sumário

Capítulo 1 – INTRODUÇÃO

Vitória Akemi Corrêa Arakaki – RA: 422101990

A gestão de projetos de Tecnologia da Informação (TI) requer soluções que combinem segurança da informação, agilidade operacional e controle eficiente do ciclo de vida dos dados. Em ambientes colaborativos, nos quais múltiplos *stakeholders* compartilham arquivos estratégicos e sensíveis, o risco de exposição indevida, vazamento ou retenção não autorizada de informações pode comprometer tanto a integridade do projeto quanto sua conformidade com padrões legais e regulatórios.

Este trabalho propõe o desenvolvimento de uma aplicação web para o envio e recebimento de arquivos com armazenamento temporário em nuvem, concebida especificamente para atender às demandas de gestão segura de dados em projetos de TI. A solução possibilita o compartilhamento controlado de arquivos, com armazenamento transitório e exclusão automática após o acesso ou clonagem, assegurando que apenas cópias autorizadas permaneçam disponíveis aos usuários.

Essa abordagem contribui diretamente para a governança da informação, mitigando vulnerabilidades, otimizando o uso de recursos computacionais e promovendo rastreabilidade completa das operações realizadas sobre os arquivos. Além disso, a aplicação foi concebida em conformidade com a Lei Geral de Proteção de Dados (LGPD), reforçando princípios de privacidade, transparência e segurança jurídica no tratamento de dados pessoais e corporativos.

A adoção dessa solução em processos de gestão de projetos de TI amplia o controle sobre os documentos compartilhados, melhora a comunicação entre equipes e reduz riscos operacionais, fortalecendo a maturidade dos processos de governança e segurança da informação nas organizações.

Capítulo 1.1 – Justificativa

Vitória Akemi Corrêa Arakaki – RA: 422101990

Com o avanço da transformação digital e a crescente adoção de infraestruturas em nuvem, a segurança no compartilhamento de arquivos tornou-se um elemento crítico em contextos corporativos, acadêmicos e pessoais. A transmissão de informações confidenciais por meios digitais exige mecanismos robustos de autenticação, criptografia e controle de acesso, capazes de garantir a integridade, a confidencialidade e o rastreamento de dados durante todo o seu ciclo de vida.

Nesse contexto, o desenvolvimento de uma aplicação que permita o envio e recebimento de arquivos com armazenamento temporário e exclusão automática surge como uma solução eficaz para mitigar riscos relacionados à exposição indevida de informações, vazamentos acidentais ou uso não autorizado de documentos.

Além de aprimorar a segurança informacional, a proposta contribui para a eficiência computacional, evitando o acúmulo desnecessário de dados em servidores e promovendo práticas mais sustentáveis e escaláveis de gestão de informação. Sua aplicabilidade é ampla, abrangendo cenários como transmissão de documentos jurídicos, relatórios corporativos, trabalhos acadêmicos e arquivos pessoais, em que a confidencialidade e o controle de acesso são imprescindíveis.

Capítulo 1.2 – Objetivos

Vitória Akemi Corrêa Arakaki – RA: 422101990

Desenvolver uma aplicação web segura para o envio e recebimento de arquivos digitais com armazenamento temporário em nuvem, que realize a exclusão automática dos dados após o acesso e clonagem, priorizando segurança, rastreabilidade e eficiência no gerenciamento da informação em projetos de TI.

Objetivos Específicos

- Implementar uma **estrutura de armazenamento temporário** em nuvem com descarte automatizado dos arquivos após o uso.
- Desenvolver **mecanismos de autenticação e controle de acesso** para garantir a integridade e a confidencialidade dos dados.
- Criar **funcionalidades de rastreabilidade e auditoria (logs)** que permitam monitorar o ciclo de vida completo dos arquivos compartilhados.
- Integrar **protocolos de comunicação segura** (HTTPS/TLS) para transferência criptografada de dados entre usuários.
- Realizar **testes funcionais, de desempenho e segurança** com ferramentas de mercado, assegurando a confiabilidade do sistema.
- Avaliar a **conformidade legal** da aplicação com a **Lei Geral de Proteção de Dados (LGPD)** e outras normas correlatas de segurança digital.

Capítulo 1.3 – Metodologia

Vitória Akemi Corrêa Arakaki – RA: 422101990

O desenvolvimento da aplicação seguiu uma **metodologia de engenharia de software** estruturada, priorizando **segurança, escalabilidade, usabilidade e conformidade legal**. As etapas metodológicas são:

1. Levantamento de Requisitos: Identificação dos requisitos funcionais e não funcionais, com foco em segurança, controle de acesso, exclusão automatizada e aderência à LGPD.
2. Seleção de Tecnologias: Utilização de tecnologias modernas e amplamente consolidadas no mercado:
    - **Frontend:** *HTML5, CSS3, JavaScript (frameworks React ou Vue.js).*
    - **Backend:** *Node.js (Express)* ou *Python (Django/Flask)*.
    - **Banco de dados:** *MongoDB* ou *PostgreSQL*;
    - **Armazenamento em nuvem:** *AWS S3*, *Firebase Storage* ou *Azure Blob Storage;*
    - **Segurança:** Autenticação *JWT*, criptografia *AES* e controle de sessões seguras.
3. Modelagem e Arquitetura: A arquitetura segue o padrão cliente-servidor com separação de camadas, adotando diagramas UML (casos de uso, classes e sequência) para representação estrutural e funcional do sistema.
4. Implementação: Desenvolvimento modular com controle de versão em *Git*, abrangendo rotinas de *upload, download,* clonagem e exclusão automatizada de arquivos.
5. Testes e Validação: Aplicação de testes funcionais, de segurança e de desempenho, utilizando ferramentas como *Postman, Jest e OWASP ZAP*, para garantir a robustez e a resiliência do sistema.
6. Documentação Técnica: Elaboração de documentação completa incluindo arquitetura, código-fonte, APIs, procedimentos de segurança e resultados de testes, visando facilitar manutenção e auditoria futura.

Capítulo 1.4 - Fundamentação Teórica

Vitória Akemi Corrêa Arakaki – RA: 422101990

A fundamentação teórica deste trabalho baseia-se em quatro eixos principais: computação em nuvem, segurança da informação, engenharia de software e proteção de dados pessoais.

A computação em nuvem, segundo *Armbrust et al. (2010),* é um modelo de fornecimento de recursos computacionais sob demanda, caracterizado pela elasticidade, escalabilidade e otimização de custos, tornando-se essencial para o armazenamento e processamento de grandes volumes de dados.

Em termos de segurança da informação, adotam-se os princípios fundamentais de confidencialidade, integridade e disponibilidade (CIA), conforme *Stallings (2017*). A aplicação proposta incorpora esses pilares por meio de autenticação segura, criptografia de dados em repouso e em trânsito, além da exclusão automatizada de arquivos sensíveis.

A engenharia de software sustenta o processo de desenvolvimento por meio de metodologias ágeis, como o Scrum, que promovem entregas incrementais, feedback contínuo e alta adaptabilidade às mudanças de requisitos *(Pressman, 2016).* Aliam-se a essas práticas os princípios de DevSecOps, que integram aspectos de segurança desde as etapas iniciais do ciclo de vida do software.

Por fim, a *Lei Geral de Proteção de Dados (Lei nº 13.709/2018)* orienta a conformidade legal da aplicação, garantindo que o tratamento de dados pessoais respeite os princípios da finalidade, necessidade, transparência e segurança, conforme estabelecido pela legislação brasileira.

Capítulo 1.5 – Resultados esperados

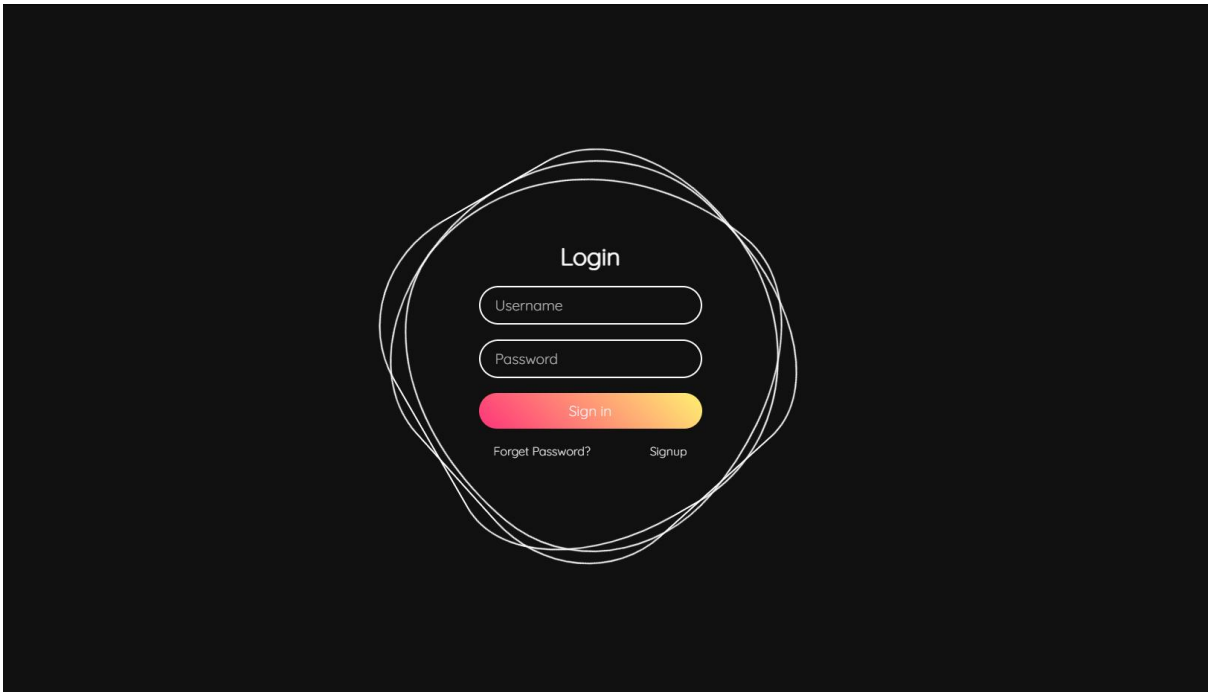
Vitória Akemi Corrêa Arakaki – RA: 422101990

- Elevação do nível de segurança e controle no compartilhamento de arquivos digitais.
- Exclusão automática dos dados após acesso, reduzindo riscos de retenção indevida. Rastreabilidade completa das ações realizadas sobre os arquivos (auditoria e logs). Conformidade com a LGPD e demais normas de segurança da informação. Desempenho satisfatório em testes funcionais e de vulnerabilidade.
- Interface intuitiva e responsiva, com experiência de usuário otimizada.
- Escalabilidade da solução, permitindo adaptação a diferentes contextos e volumes de dados.

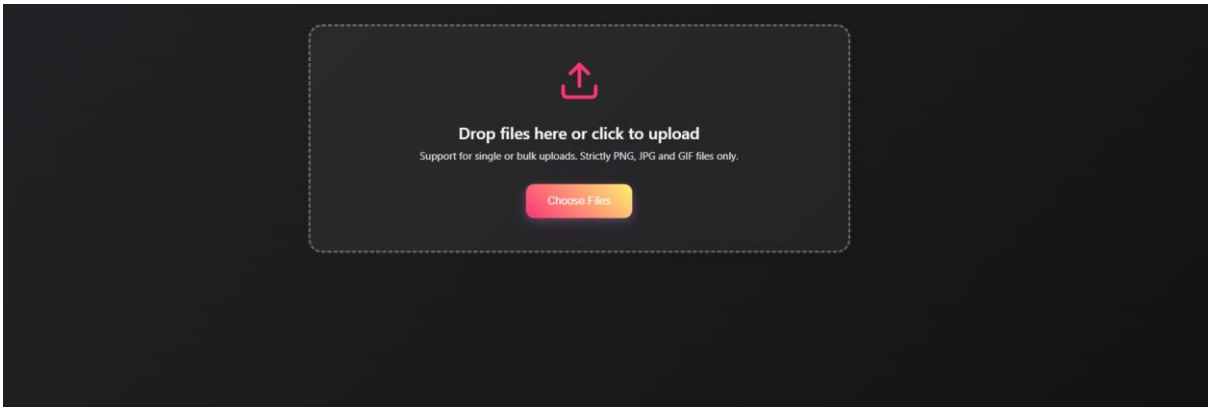
Capítulo 2 – Produção

Vitória Akemi Corrêa Arakaki – RA: 422101990

Tela de login:



Tela de upload dos arquivos:



Capítulo 3 – Requisitos do sistema

Vitória Akemi Corrêa Arakaki – RA: 422101990

3.1 Requisitos funcionais (RF)

Os requisitos funcionais descrevem **o que o sistema deve fazer**, isto é, as funções e comportamentos esperados da aplicação.

ID	Descrição
RF01	O sistema deve permitir o upload de arquivos por usuários autenticados.
RF02	O sistema deve armazenar os arquivos em um servidor em nuvem.
RF03	O sistema deve atribuir um tempo de validade para cada arquivo enviado.
RF04	O sistema deve excluir automaticamente os arquivos do servidor após o prazo de validade ou após o primeiro acesso/download.
RF05	O sistema deve permitir o download seguro de arquivos compartilhados, mediante autenticação ou link temporário.
RF06	O sistema deve gerar links temporários (com token de segurança) para compartilhamento de arquivos.
RF07	O sistema deve permitir o rastreamento de atividades, registrando logs de upload, download, acesso e exclusão.
RF08	O sistema deve implementar autenticação de usuários via login e senha, com tokens JWT.
RF09	O sistema deve permitir o registro (cadastro) de novos usuários e a recuperação de senha.
RF10	O sistema deve disponibilizar uma interface web responsiva, acessível em navegadores desktop e mobile.
RF11	O sistema deve exibir alertas e notificações quando um arquivo estiver prestes a expirar.
RF12	O sistema deve permitir que o administrador visualize relatórios de auditoria, contendo data, hora e usuário de cada ação.

3.2 Requisitos Não Funcionais (RNF)

Os requisitos não funcionais definem **qualidades e restrições técnicas** do sistema, relacionadas ao desempenho, segurança, usabilidade, confiabilidade, entre outros.

ID	Descrição
RNF01	O sistema deve seguir os princípios da LGPD, garantindo confidencialidade, integridade e finalidade dos dados pessoais.
RNF02	O sistema deve utilizar criptografia AES-256 para dados armazenados e TLS 1.3 para comunicações.
RNF03	O tempo máximo de resposta do servidor para operações críticas (upload/download) deve ser inferior a 5 segundos em condições normais de rede.
RNF04	O sistema deve ter disponibilidade mínima de 99% (uptime), conforme boas práticas de cloud computing.
RNF05	A aplicação deve ser compatível com os navegadores modernos, como Chrome, Firefox e Opera.
RNF06	O código-fonte deve seguir boas práticas de modularização, versionamento (Git) e padronização de código (ESLint/PEP8).
RNF07	A interface deve ser intuitiva, acessível e responsiva, utilizando frameworks modernos (React ou Vue.js).
RNF08	O sistema deve ser escalável horizontalmente, suportando aumento no volume de usuários e dados.
RNF09	O sistema deve registrar logs de auditoria em formato padronizado (JSON) com armazenamento seguro.
RNF10	O sistema deve implementar testes automatizados para validação funcional e de segurança.
RNF11	O sistema deve respeitar o princípio de mínimo privilégio, limitando o acesso de cada usuário ao necessário.
RNF12	O sistema deve possuir documentação técnica completa, incluindo APIs, arquitetura e políticas de segurança.

3.3 Requisitos de Ambiente

- **Sistema Operacional do Servidor:** Windows ou Linux.
- **Servidor Web:** Apache.
- **Banco de Dados:** PostgreSQL ou MongoDB.
- **Armazenamento em Nuvem:** AWS S3, Firebase Storage ou Azure Blob.
- **Linguagem de Programação:** Node.js (JavaScript/TypeScript) ou Python.
- **Framework Frontend:** React.js ou Vue.js.
- **Controle de Versão:** Git/GitHub.

3.4 Requisitos de Segurança e Conformidade

- Conformidade integral com a **Lei nº 13.709/2018 (LGPD)**.
- Implementação de **criptografia ponta a ponta** entre cliente e servidor.
- Registro e monitoramento contínuo de **logs de acesso e eventos críticos**.
- Políticas de **autenticação multifatorial (2FA)** opcionais.
- Backup automatizado dos metadados e logs em intervalos regulares.

Capítulo 4 – Desenvolvimento Orientado a Objetos

Vitória Akemi Corrêa Arakaki – RA: 422101990

Link do repositório do projeto: API_Cloud

Capítulo 5 – Conclusão

Vitória Akemi Corrêa Arakaki – RA: 422101990

O desenvolvimento da aplicação web para compartilhamento seguro de arquivos com armazenamento temporário em nuvem demonstrou a viabilidade técnica e conceitual de uma solução voltada à gestão eficiente, segura e rastreável de dados em projetos de Tecnologia da Informação. A proposta atendeu aos objetivos definidos, oferecendo um mecanismo que alia agilidade na troca de informações com garantias de confidencialidade e conformidade legal.

A implementação do armazenamento temporário e da exclusão automática de arquivos após o acesso ou clonagem contribui significativamente para a redução de vulnerabilidades e riscos de exposição indevida, fortalecendo a governança da informação e o cumprimento dos princípios da LGPD. Tais práticas reforçam o compromisso com a segurança digital, um requisito essencial em contextos corporativos e acadêmicos que lidam com dados sensíveis.

Do ponto de vista técnico, a aplicação adota uma arquitetura moderna, escalável e modular, sustentada por boas práticas de engenharia de software e DevSecOps, o que facilita sua manutenção, evolução e integração com outros sistemas. Os mecanismos de autenticação, criptografia e rastreamento de logs garantem confiabilidade e transparência nas operações realizadas pelos usuários.

Conclui-se que a solução proposta não apenas atende a uma necessidade prática da gestão de projetos de TI, mas também representa um avanço em termos de maturidade organizacional e cultura de segurança da informação. Além disso, sua flexibilidade tecnológica e seu foco em conformidade a tornam aplicável a diversos contextos — desde o compartilhamento de documentos corporativos até a gestão acadêmica e jurídica.

Como trabalhos futuros, recomenda-se a ampliação das funcionalidades de auditoria e controle de acesso, a integração com serviços de autenticação corporativa (Single Sign-On) e a adoção de algoritmos de criptografia avançada, visando aprimorar ainda mais a robustez e a escalabilidade da aplicação.