

# **Trabalho A1 - Modelos, Métodos e Técnicas em Engenharia de Software**

**Gustavo Burgos<sup>1</sup>, Jonas Ceccon<sup>1</sup>, Juan Rodrigues<sup>1</sup>, Luis Oliveira<sup>1</sup>, Nicolle Brasil<sup>1</sup>**

<sup>1</sup>Campus Tancredo Neves (TCN) – Universidade Salvador (UNIFACS)  
Salvador – BA – Brasil

12723115582@ulife.com.br, 12723212051@ulife.com.br, 12723115108@ulife.com.br, 12723131891@ulife.com.br, 12723119076@ulife.com.br

## **1. Introdução**

A organização de senhas é essencial para a preservação da segurança digital, entretanto muitos usuários enfrentam dificuldades nesse processo. Neste contexto, esta pesquisa propõe uma aplicação que facilita a criação e a organização de senhas, ao mesmo tempo que fortalece a segurança. A aplicação coloca em prática um modelo de questionamento para gerar senhas de modo específico para cada usuário com base no domínio de cada servidor, complementando com uma camada extra de segurança que dificulta a violação de múltiplas contas em caso de tentativas de acesso por usuários não autorizados. Ao associar a geração de senhas com informações contextualizadas, a aplicação assegura a integridade digital dos usuários, proporcionando uma abordagem conveniente e eficiente para gerir senhas, sem comprometer a segurança das informações pessoais dos usuários

## **2. Requisitos**

### **2.1 Requisitos Funcionais**

- O sistema deve ser capaz de armazenar senhas de forma segura em um cofre protegido por criptografia
- O sistema deve ser capaz de criar senhas de difícil acesso e exclusivas para cada site e aplicativo
- O sistema deve ser capaz de organizar as senhas por tipo de sites e categorias classificadas pelo usuário
- O sistema preenche automaticamente as senhas em sites e aplicativos
- O sistema poderá sincronizar as informações com todos os dispositivos autorizados pelo usuário.
- O sistema deve oferecer uma autenticação de 2 fatores para todos os usuários, tendo assim um maior nível de segurança da conta

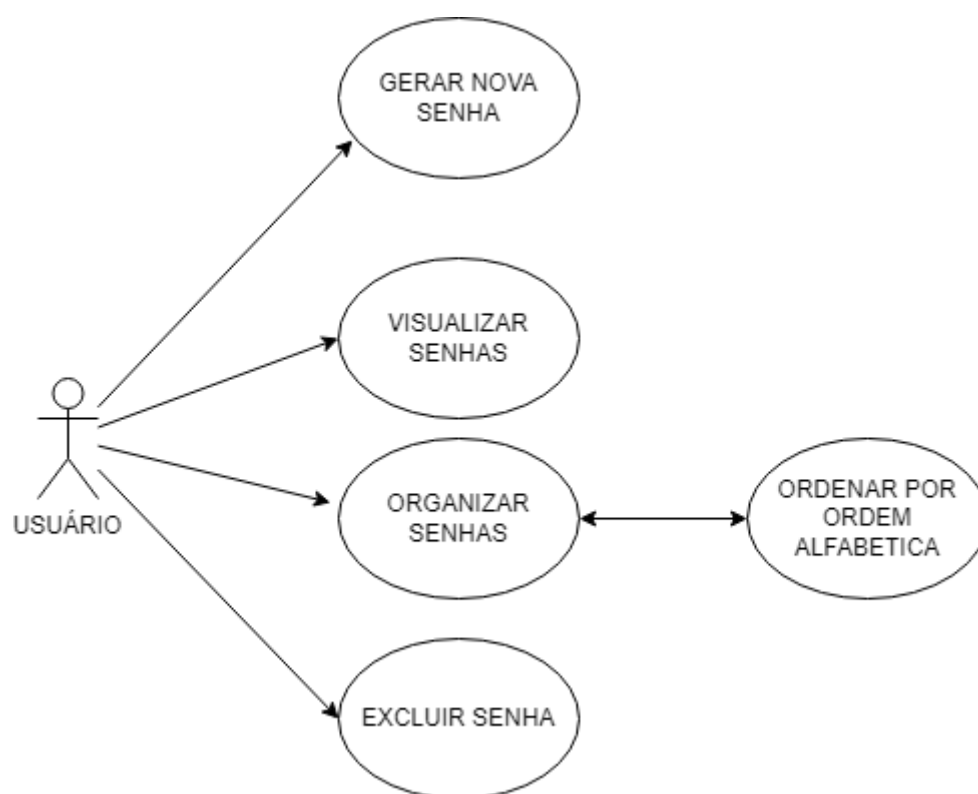
### **2.2 Requisitos não funcionais**

- O sistema deve fornecer uma interface intuitiva e de fácil acesso as informações inseridas pelo usuário
- Deve-se garantir que o sistema responda rapidamente às solicitações dos usuários, mesmo sob carga pesada.
- sistema deve garantir a proteção da privacidade dos usuários e suas informações pessoais
- O sistema deve assegurar que sempre estará disponível para os usuários sempre que necessário, com o menor tempo de inatividade
- O sistema deve ter a capacidade de dimensionar o sistema para lidar com muitos usuários e senhas.
- O sistema deve se recuperar de falhas de forma rápida e protegendo os dados de seus usuários

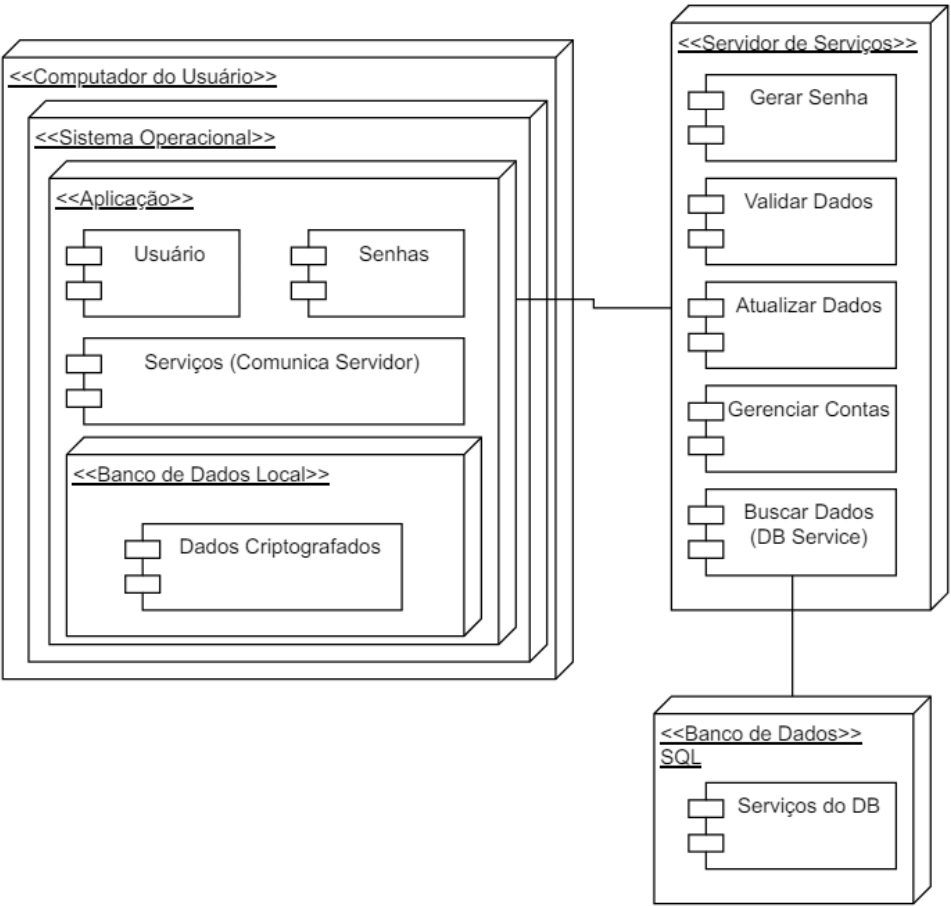
### **3. Regras de Negócio**

- Armazenamento seguro de senhas → todas as senhas são armazenadas de forma segura, sendo utilizadas proteções com criptografia contra malware e acesso não autorizados por usuários desconhecidos
- Utilização de senhas fortes → o software deve permitir somente as senhas geradas atendam a critérios de segurança como uso de letras maiúsculas, letras minúsculas e caracteres especiais
- Backup para recuperação de senhas → deve haver uma aplicação que de backup para recuperação de senhas para caso haja falha no sistema ou perda de acesso ao software
- Gerenciamento de acesso por terceiros → deve ter uma funcionalidade que gerencie o acesso podendo permitir ou negar o acesso de terceiros a contas protegidas pelo software, como aplicativos infectados que possam ter acessos aos dados guardados
- Monitoramento de vulnerabilidade → o software deve oferecer mecanismos para monitorar e alertar sobre possíveis vulnerabilidades em contas com senhas fracas, reutilizadas ou comprometidas em violações de dados

#### 4. Diagrama de arquitetura lógica



5. Diagrama de arquitetura física



6. Board ágil

