**Levantamento de Requisitos – Projeto SecureBox (Criptografia Simétrica)**

**1. Objetivo do Sistema**

Desenvolver uma aplicação que permita a criptografia e descriptografia de arquivos utilizando criptografia simétrica (AES), com foco em segurança, integridade de dados, portabilidade e estruturação profissional do código.

**2. Requisitos Funcionais (RF)**

| **Código** | **Requisito** |
| --- | --- |
| RF01 | O sistema deve permitir ao usuário criptografar arquivos com uma senha. |
| RF02 | O sistema deve permitir ao usuário descriptografar arquivos utilizando a mesma senha. |
| RF03 | O sistema deve utilizar o algoritmo AES (Advanced Encryption Standard) no modo GCM. |
| RF04 | O sistema deve derivar a chave criptográfica a partir de uma senha utilizando PBKDF2. |
| RF05 | O sistema deve gerar automaticamente salt e nonce para cada operação de criptografia. |
| RF06 | O sistema deve armazenar salt, nonce e tag de autenticação junto com o arquivo criptografado. |
| RF07 | O sistema deve verificar a integridade dos dados durante a descriptografia. |
| RF08 | O sistema deve exibir mensagens claras para operações concluídas ou falhas. |
| RF09 | O sistema deve funcionar via linha de comando. |
| RF10 | O sistema deve permitir a seleção do arquivo de entrada e nome do arquivo de saída. |

**3. Requisitos Não Funcionais (RNF)**

| **Código** | **Requisito** |
| --- | --- |
| RNF01 | O sistema deve ser desenvolvido em Python 3.10 ou superior. |
| RNF02 | O sistema deve utilizar bibliotecas confiáveis e seguras, como cryptography. |
| RNF03 | O código deve seguir boas práticas de desenvolvimento, como modularização e clareza. |
| RNF04 | O desempenho deve ser aceitável para arquivos de até 100 MB. |
| RNF05 | O sistema deve ser compatível com Windows, Linux e macOS. |
| RNF06 | As mensagens exibidas ao usuário devem estar em português. |

**4. Requisitos de Segurança (RS)**

| **Código** | **Requisito** |
| --- | --- |
| RS01 | A chave de criptografia deve ser derivada por PBKDF2HMAC com salt aleatório e seguro. |
| RS02 | A senha do usuário não deve ser armazenada nem exibida em texto plano. |
| RS03 | A integridade dos dados deve ser validada utilizando a tag de autenticação do AES-GCM. |
| RS04 | O sistema deve rejeitar descriptografias com senha incorreta, com mensagens de erro claras. |

**5. Escopo do MVP (Produto Viável Inicial)**

* Suporte a qualquer tipo de arquivo
* Interface por linha de comando
* Armazenamento de salt, nonce e tag diretamente no arquivo criptografado
* Separação do código em módulos: entrada do usuário, criptografia e utilidades.