# Aplicação de Criptografia AES no Projeto OrganizAi

## 1. Justificativa da Criptografia

O algoritmo escolhido para proteger os dados sensíveis do projeto foi o AES (Advanced Encryption Standard), um padrão amplamente adotado por organizações como o NIST (National Institute of Standards and Technology). AES é um algoritmo de criptografia simétrica, eficiente, seguro e ideal para aplicações que exigem confidencialidade de dados como endereços, documentos ou identificadores.

No projeto, os campos AddressOrig e AddressDest foram criptografados antes de serem armazenados no banco de dados SQLite. A criptografia foi aplicada utilizando o modo CBC (Cipher Block Chaining) com chave de 256 bits derivada por SHA-256. A descriptografia ocorre somente na leitura dos dados, garantindo assim segurança e confidencialidade.

## 2. Explicação Resumida do Algoritmo AES

AES (Advanced Encryption Standard) é um algoritmo de cifra por blocos com chave simétrica, ou seja, usa a mesma chave para criptografar e descriptografar. Ele opera em blocos de 128 bits e suporta chaves de 128, 192 ou 256 bits. O algoritmo aplica uma série de transformações nos dados, como substituições, permutações, mistura de colunas e adição de chave, em múltiplas rodadas, tornando os dados praticamente irreversíveis sem a chave correta.

## 3. Contexto de Aplicação no Projeto

A criptografia foi implementada diretamente no notebook Jupyter, utilizando a biblioteca PyCryptodome. Os dados criptografados foram armazenados em uma nova tabela no banco (DADOSUBER\_CRYPT), e demonstramos também como realizar a leitura e descriptografia corretamente para recuperação da informação.