**Memorial Descritivo – Criptografia**

**Empresa: EiTruck**

**Aplicativo: Ei Truck**

**Integrantes:**

• Ana Clara Araújo Costa

• Beatriz Dias Inácio

• Giovanna Quirino

• Igor Eduardo Quinto

• Samuel Pimenta Hironimus

• Verena Marostica Marcelino

**Turma:** 1ª Série J – Tech

O método de criptografia utilizado para “esconder” as senhas no banco de dados desse projeto foi implementado por meio da biblioteca **bcrypt**, reconhecida por sua segurança no armazenamento de senhas. O objetivo principal é proteger as credenciais dos usuários e evitar que senhas sejam armazenadas em texto puro no banco de dados.

**Implementação**

A função **criptografar(senha)** que foi utilizada no python**,** é responsável por transformar a senha original em um *hash* seguro. O processo ocorre em duas etapas principais:

Gera um salt(bcrypt.gensalt())**:** O salt é um valor aleatório criado para cada senha. Ele serve para garantir que senhas idênticas gerem hashes diferentes.

Geração do hash(bcrypt.hashpw())**:** A função “junta” a senha e o salt, e o resultado é uma sequência de caracteres ilegível, no caso a senha criptografada. O valor é então convertido em string com decode('utf-8') para poder ser armazenado no banco de dados.

**Autenticação**

Para a autenticação da senha, a função verificar\_senha(senha\_digitada, senha\_criptografada) funciona da seguinte forma: O bcrypt aplica o mesmo processo de hash na senha digitada e compara o resultado com o hash armazenado. Se forem compatíveis, a função retorna True, caso contrário, False.

**Por que é um método seguro?**

O bcrypt é considerado um método seguro já que utiliza salt único para cada senha, é computacionalmente lento de propósito, então dificulta ataques de força bruta(o invasor tenta todas as combinações possíveis até achar a certa) e não permite reversão do hash, ou seja, não tem como recuperar a senha original.

--------------------------------------------------------------------------------------------------------

**Fontes utilizadas como auxílio para produção deste memorial**

Documentação PyPi:

<https://pypi.org/project/bcrypt/>

Repositório no GitHub para auxílio de uso:

<https://github.com/pyca/bcrypt>