



## ATIVIDADE FORMATIVA: SEMANA 5

---

### Funções *Hash* Criptográficas

A atividade formativa proposta para esta semana visa explorar os conceitos de funções hash criptográficas. O propósito da atividade é utilizar, de maneira prática, algoritmos de funções hash criptográficas para garantir a integridade da informação.

Acesse o arquivo `Semana5_AtividadeFormativa.pdf` para ler a descrição completa da atividade.

### Cenário:

No banco de Tóquio informações sigilosas acabaram sendo expostas, em alguns dos sistemas internos a senha trafegava em aberto (sem criptografia), não há garantia que os dados não foram modificados. Visando garantir a integridade dos dados no novo servidor, deverá ser utilizado funções hash criptográficas que deverão ser aplicadas sobre todos os dados sensíveis. Deste modo, será reforçado este mecanismo de segurança.

### Especificação da Atividade:

Nesta atividade você deverá desenvolver um sistema de autenticação do banco de Tóquio. O programa deve ser escrito na linguagem Python, implementar duas funcionalidades: cadastrar e autenticar o usuário. O programa deve atender os seguintes requisitos:

1. Fornecer um menu para o usuário: cadastrar ou autenticar
2. Cadastrar o usuário;
  - a. Solicitar as informações do usuário pelo console;
  - b. As informações do usuário deve conter o nome, login e senha;
  - c. Armazenar a senha utilizando o algoritmo de função *hash* MD5;
  - d. As informações do usuário devem ser gravadas em um arquivo ".txt";
3. Autenticar o usuário;
  - a. Solicitar as informações do login e senha do usuário pelo console;
  - b. Efetuar a leitura do arquivo .txt onde estão foram salvas as informações dos usuários;
  - c. Verificar se o login está cadastrado;
  - d. Validar se o login foi cadastrado;
  - e. Para condição onde o login não foi cadastrado, fornecer a mensagem: "Autenticação Inválida!!";
  - f. Ao localizar o login do usuário aplicar a função hash MD5 sobre a senha fornecida pelo usuário;
  - g. Verificar se a senha fornecida é igual a senha armazenada no arquivo ".txt";
  - h. Para condição da senha serem diferentes, fornecer a mensagem: "Autenticação Inválida!!";



- i. Caso a senha esteja correta, apresentar uma mensagem de “bem-vindo” contendo o nome do usuário.

### Dicas:

O código a seguir demonstra o processo necessário para utilizar a função MD5 na linguagem Python.

```
MD5.py ×  
1  import hashlib  
2  
3  mensagem = "Hello World!!"  
4  hash = hashlib.md5(mensagem.encode())  
5  print("Hash MD5: " + hash.hexdigest())
```