|  | | **Banco de Dados**  **Linguagem SQL**  **AC2 – Criptografia** | | |
| --- | --- | --- | --- | --- |
| *Nome do Aluno:* | | | | *RA:* |
| *Turma:* | *Série:* | | *Data:* \_\_\_/\_\_\_/\_\_\_\_\_\_ | |
| *Professor(a) Responsável:* Gustavo Bianchi Maia | | | | |
| Nota: ( ) Visto do Prof. | | | | |

**Seu objetivo é automatizar os processos de armazenamento de logins, senhas e dicas de senha e o processo de autenticação de um sistema, de forma que a utilização das informações deve se dar da seguinte maneira:**

**- Uma tabela TBL\_CTRL\_ACESSO, com os campos citados acima, com**

**- Login, não precisa nem deve ser criptografado na base**

**- Senha, deve ser armazenado com criptografia 1-WAY**

**- Dica\_senha, deve ser armazenado com criptografia 2-WAY**

**Para concluir esta atividade você precisará criar:**

**- Uma função, que receba um texto e devolva-o criptografado ( fn\_encrypt )**

**- Outra Funcão, que receba um valor criptografado e o decriptografe ( fn\_decrypt )**

**- Uma função, que receba um texto e o criptografe ( fn\_hash ) 🡪 use “SALT”**

**De forma que tais funções possam ser utilizadas nos exemplos criados para insirir valores na tabela obedecendo às recomendações.**

**Finalmente:**

**- Crie uma procedure que: dado um login e senha, devolva “1” se autenticado e “0” caso contrário.**

**- Crie uma procedure que: dado um login, devolva a dica da senha, decriptografada.**

**Preencha esta ficha de avaliação, copie e cole todos os códigos utilizados e entregue para o professor.**

**Abaixo algumas orientações passadas em sala de aula:**

Sejam as seguintes funções ( Que serão criadas na AC2 )

***--Função de criptografia***

**SELECT dbo.Fn\_encrypt('oi')**

Recebe uma string e devolve o respectivo valor criptografado em VARBINARY utilizando um algoritmo de 2 vias assimétrico de criptografia.

***--Função de decriptografia***

**SELECT dbo.Fn\_decrypt(dbo.Fn\_encrypt('oi'))**

Recebe um valor já criptografado e devolve o respectivo valor descriptografado já convertido em VARCHAR

***--Função de criptografia de HASH***

**SELECT dbo.Fn\_hash('oi')**

Recebe uma string e devolve o respectivo valor criptografado em VARBINARY utilizando um algoritmo de HASH com a utilização de um SALT ( por segurança ).

***--Criando a tabela TBL\_CTRL\_ACESSO***

**CREATE TABLE tbl\_ctrl\_acesso**

**( [login] *VARCHAR*(60) NOT NULL,**

**[senha] *VARBINARY*(max) NOT NULL,**

**[dica\_senha] *VARBINARY*(max) NULL,**

**CONSTRAINT pk\_ctrl\_acesso PRIMARY KEY ( [login] )**

**)**

***--Inserindo valores nas tabelas para testes:***

**INSERT INTO tbl\_ctrl\_acesso( [login], [senha], [dica\_senha] )**

**VALUES ( 'José', dbo.Fn\_hash('senha'),dbo.Fn\_encrypt('aquela lá') )**

**go**

***--Testando valores brutos inseridos na tabela***

**SELECT \* FROM tbl\_ctrl\_acesso**

**go**

***--Testando valores decriptografados lidos da tabela***

**SELECT [login], [senha],**

***CONVERT*(*VARCHAR*, dbo.Fn\_decrypt([dica\_senha])) AS [dica\_senha]**

**FROM tbl\_ctrl\_acesso**

**go**

Seja a seguinte procedure ( que também será criada na AC2 )

**EXEC Pr\_login @login, @senha, @result output**

Que, recebe um login e senha ( ambos varchar ) e devolve 1 se ele foi autenticado, ou seja, se aquele usuário foi cadastrado com aquela senha, e 0 caso contrário.

Exemplo de utilização:

***--testando procedure de login***

**DECLARE @result *BIT***

***--autenticado***

**EXEC Pr\_login 'josé', 'senha', @result output**

**SELECT CASE WHEN @result = 1 THEN 'Autenticado' ELSE 'Não autenticado' END**

***--não autenticado***

**EXEC Pr\_login 'josé', 'senha errada', @result output**

**SELECT CASE WHEN @result = 1 THEN 'Autenticado' ELSE 'Não autenticado' END**

**go**

Seja a seguinte procedure ( que também será criada na AC2 )

**EXEC Pr\_esqueci\_senha @login, @result output**

Que, recebe um login ( varchar ) e devolve a dica da senha decriptografada, cadastrada para aquele login.

Exemplo de utilização:

***--Testando a procedure esqueci senha***

**DECLARE @result *VARCHAR*(60)**

**EXEC Pr\_esqueci\_senha 'josé', @result output**

**SELECT 'Sua dica da senha é: "' + @result + '"'**

**go**

**Observações:**

* Avaliação individual
* Organização, clareza e legibilidade na resolução da prova serão consideradas na correção.
* A interpretação da atividade faz parte do processo de avaliação
* Qualquer tentativa de fraude, cola será punido com nota zero.
* O total desta avaliação corresponde à 1 de 5 avaliações continuadas.

**Boa Avaliação!**