Insurity Consultoria

Implementação de regras de segurança

Especificação de Requisitos de Software (SRS)

Para: Hatomus Cursos Online

Versão <1.0>

Aluno: Douglas Maciel Turma: Full-Stack 1

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO	AUTOR
20/05/2022	1.0	Desenvolvimento da documentação SRS	Douglas Maciel

3.4 Outros Requisitos

3.4.1 Requisitos de Usabilidade

3.4.2 Requisitos de Confiabilidade

3.4.3 Suportabilidade

1. Introdução

1.1 Finalidade

Implementar um modelo para proteção de senha para perfil, com a finalidade de reduzir os riscos e prevenir ameaças, garantindo o sigilo das informações e assegurando a confidencialidade dos dados, baseados em três fatores: disponibilidade, confidencialidade e integridade.

1.2 Escopo

Foi adicionado criptografia ao sistema a função, HASHBYTES, para proteger e criptografar senhas no SQL Server, respeitando a lei LGPD.

1.3 Definições, Acrônimos, e Abreviações

(SRS) Especificação de Requisitos de Software.

(LGPD) Lei Geral de Proteção de Dados Pessoais.

(SQL Server) SQL Server é um sistema gerenciador de Banco de dados.

2. Descrição Geral

Segundo a definição do Computer Security Resource Center,1 a Segurança da Informação, é: *“A proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de garantir a confidencialidade, integridade e disponibilidade.”*

Temos como objetivo reduzir os riscos e prevenir ameaças, garantindo o sigilo das informações e assegurando a confidencialidade dos dados.

Quanto maior a segurança do algoritmo, menor a chance de uma informação ser "quebrada“ ou recuperada indevidamente. Um exemplo é o **HASHBYTES**, permite trabalhar com funções criptográficas baseadas em HASH, onde uma vez codificado, não é possível obter a string original novamente

Restrições: A senha do usuário será criptografada, e não terá como ser visualizada, nem pelo sistema, nem pelo usuário. Terá apenas a comparação criptográfica da mesma pelo sistema.

3. Requisitos Específicos

3.1 Requisitos Funcionais

3.1.1 Requisito Funcional 1

Sistema de login com validação de senha do usuário.

3.1.2 Requisito Funcional 2

Utilizar criptografia no banco de dados para proteção dos dados dos usuários.

3.2 Requisitos de Performance

3.2.1 Requisito de Performance 1

O tempo de resposta deve ser em média 5 segundos.

3.3 Atributos do Sistema de Software

3.3.1 Restrições do Design

3.3.1.1 Restrição de Design Um

Visto que o sistema utiliza a criptografia do tipo **HASHBYTES,** seria interessante solicitar aos desenvolvedores Front-End, que atualizem o retorno das senhas para uma visualização agradável.

3.3.2 Interfaces

3.3.2.1 Interface de Usuário

O HASHBYTES, tem como retorno algo do tipo: 0x741238C01D9DB821CF171BF61D72260B998F7C7881D90091099945E0B9E0

Pode-se alterar a visualização da Interface do Usuário para algo como : **********

3.4 Outros Requisitos

3.4.1 Requisitos de Usabilidade

O sistema está pronto para uso, não interferindo na usabilidade do usuário.

Salvo o retorno da senha que precisa ser corrigido pelo Front-End.

3.4.2 Requisitos de Confiabilidade

A função HASHBYTES implementada no SQL Server, permite trabalhar com funções criptográficas baseadas em HASH, onde uma vez codificado, não é possível obter a senha original novamente.

Essa forma de validação é considerada uma das mais seguras na criptografia, uma vez que a complexidade da codificação é muito maior e dificulta ataques hackers para quebrar a senha codificada.

3.4.3 Suportabilidade

O sistema foi preparado para suportar até 500 conexões por segundo, pode ter instabilidade ou até a queda do sistema caso ultrapasse.