DBC COMPANY

Safety Soft

Solução de T.I. para área de saúde

API RESTful do sistema back-end para integração.

Agendamento e gestão de consulta

Apresentado por:
Matheus Palermo, Pedro Sousa e Thassio Vagner.

27/03/2023

Trabalho final - módulo 03.

ESTRUTURA

- Usuário Administrativo - tem acesso a todas funcionalidades do sistema.
- Cliente - possui informações pessoais básicas e de login, esse pode ter algum Convênio.
- Convênio - para o cadastro no Cliente, podendo ter algum abatimento no valor da consulta.
- Médico - possui informações pessoais básicas e de login, deve ter necessariamente alguma Especialidade.
- Especialidade - para registrar a atuação e variante do valor de consulta dos médicos.
- Agendamento - é usado para registrar uma consulta de um paciente (Cliente) com um médico.

Diferenças de permissões:

- Qualquer pessoa consegue: criar um login, se autenticar, trocar sua senha (estando logado), redefinir sua senha (sem estar logado), se cadastrar como médico ou cliente.
- Um Administrador faz operações de CRUD (create, read, update e delete) em qualquer classe, especialmente: Convênio, Especialidade e Agendamento. Ou seja, somente ele faz agendamentos.
- Um Cliente e um Médico podem somente: atualizar suas informações de cadastro, verificar suas informações e verificar seus agendamentos.

Destaques desta versão:

- Sistema de autenticação e segurança, bem como diferenciação de acessos e sistema para login (com criptografia de senhas e recursos para recuperação de acesso).
- Valor da consulta é calculado e incluído no agendamento, com base na especialidade do médico e desconto de convênio do cliente.
- Envio de e-mails nos casos em que: se cria um usuário, se inlui, altera ou exclui um Agendamento (enviado tanto ao médico quanto ao Cliente), se solicita um código para redefinir senha e ao ter alterado a senha.
- Retorno de informações adicionais do endereço coletadas através da pesquisa de CEP por uma comunicação com a API pública do site viacep.com.br.

Como funciona o algoritmo
BCrypt

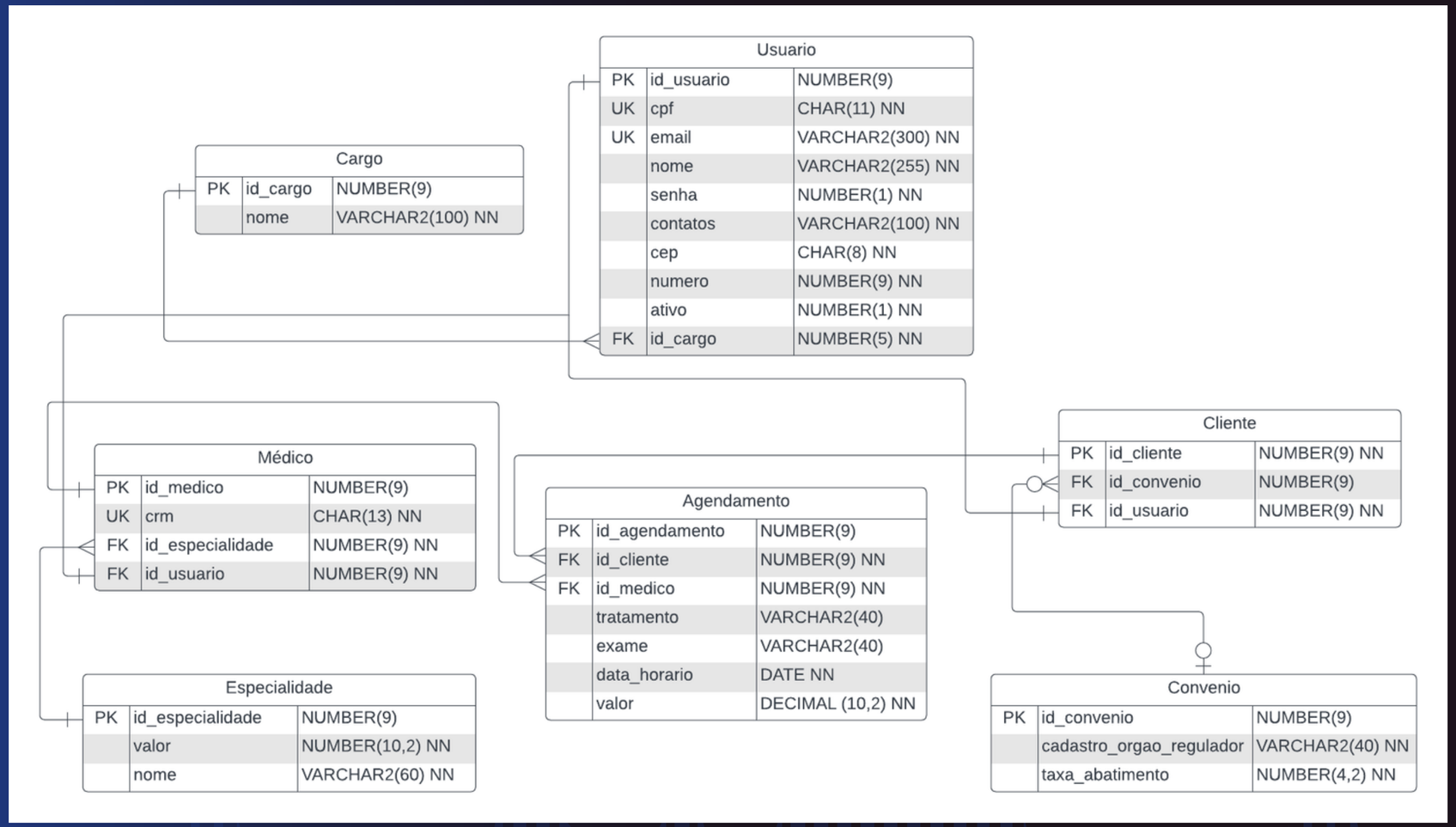
$2a$10$m1RZN932EgtR9BmYIPNj6.z1nSp0xeWovpO1gQUq2YwAH.GDQyGxm

1. O algoritmo recebe uma senha como entrada.
2. Em seguida, ele gera aleatoriamente um "salt" (um valor aleatório que é adicionado à senha antes de ser criptografado).
3. O bcrypt, em seguida, executa uma função de hash chamada Blowfish várias vezes (o número de vezes depende do "custo" configurado). O resultado é um hash da senha original e do salt.
4. O resultado final é uma string que contém o hash da senha original, o salt e algumas outras informações. Essa string é geralmente chamada de "hash da senha".
5. Quando um usuário faz login, o bcrypt repete o processo com a senha que o usuário fornece, usando o mesmo salt que foi usado para criar o hash original da senha. Se o hash resultante for igual ao hash original armazenado, a senha é considerada válida.

Explicado pelo ChatGPT

Diagrama Entidade Relacionamento

(como os dados serão armazenados)



DBC COMPANY

Ambientação

- um pouco de demonstração do funcionamento.

Um pouco de código...

- alguns destaques de soluções implementadas.

DÚVIDAS?

Agradecemos a atenção.

DBC COMPANY