Bcrypt PasswordEncoder

- O BCrypt, criado em 1999 por Niels Provos e David Mazières, é uma alternativa segura aos algoritmos de hash de senha como MD5 e SHA-1.
- Utilizando um hash iterativo e um sal aleatório, ele gera hashes de senha resistentes a ataques.
- Sua segurança é alta devido à sua resistência a ataques de força bruta e rainbow tables.
- Apesar do custo computacional mais elevado e do armazenamento de hashes mais longos, o BCrypt é amplamente utilizado em aplicações web e frameworks de segurança. Variantes como bcrypt2 e scrypt oferecem melhorias em segurança e desempenho.
- Antes do BCrypt, MD5 e SHA-1 eram comuns, mas menos seguros. Ajustar o custo de computação do BCrypt é essencial para equilibrar segurança e desempenho.