**Clara APP**

| **GRUPO 01 - CLARA APP** | |
| --- | --- |
| **Integrante** | **RA** |
| Beatriz Portela | 22023095 |
| Breno Barbosa | 22023071 |
| Esdras Mendes | 22023038 |
| Lucas Navarro | 22023179 |
| Lucas Silva | 22023562 |
| Jacqueline Nakirimoto | 22023521 |

1 – Login para acessar a sessão de usuário.

**b) Qual o algoritmo escolhido para a criptografia**

Escolhemos utilizar o “Argon2”.

**c) Qual a razão pela escolha do algoritmo**

Para o sistema de login, nossa escolha foi o algoritmo "Argon2".

Essa decisão foi tomada considerando alguns principais pontos, sendo eles:

* Sua notável resistência a ataques
* Ampla aceitação na comunidade de segurança
* Flexibilidade que ele oferece para a personalização de parâmetros.

Essa flexibilidade nos permite ajustar as métricas de segurança de acordo com as necessidades específicas de cada acesso ou fase do projeto. O "Argon2" é uma escolha sólida que combina segurança com adaptabilidade, assegurando que as senhas dos usuários estejam bem protegidas em nosso sistema.

2 – Salvar e armazenar as aferições de diabetes

**b) Qual o algoritmo escolhido para a criptografia**

Escolhemos utilizar o “AES (Advanced Encryption Standard)”.

**c) Qual a razão pela escolha do algoritmo**

Para armazenar dados mais sensíveis, como aferições de diabetes, optamos pela utilização do algoritmo de criptografia "AES", devido à sua eficácia comprovada e segurança. Uma característica significativa do AES é sua flexibilidade, permitindo ajustes no tamanho das chaves, que podem variar de 128 bits a 256 bits.

A escolha do AES foi baseada em uma análise, considerando alguns fatores:

Capacidade de integração do AES com outros serviços e frameworks, sua extensa quantidade de testes e aprovações em todo o mundo, que comprovam seu poder e eficiência, além do desempenho notável que ele oferece.

Fatores decisivos para a seleção do AES para criptografar esses dados:

* Segurança
* Adaptabilidade
* Confiabilidade
* Adequação para proteger informações críticas, como as aferições de diabetes.

Esses fatores foram comprovados com performance que atende os requisitos para a proteção dos dados.