**GoChat**

**Hecho:**

* Funcionalidad:
  + Login/Registro: sí que se almacenan en la base de datos.
  + Chats (público y privado): sólo con usuarios que estén logueados, no hay persistencia de los mensajes.
  + Ver y buscar perfiles usuario: de todos los usuarios almacenados en la base de datos.
* Seguridad:
  + Autenticación seguro: está hecho con hash. Si tenemos tiempo miraremos de hacerlo con Hash+Sal o PBKDF+Sal.

**Por hacer:**

* Funcionalidad:
  + Sincronización de mensajes entre usuarios: si tenemos tiempo miraremos si utilizar el mutex para la sincronización entre usuarios.
* Seguridad:
  + Cifrado en tiempo real: tenemos pensado hacerlo con ChaCha.
  + Optimización de privacidad: tenemos pensado hacerlo cifrando y descifrando los mensajes de chat el cliente. Los datos que tendría en claro el servidor serían los mensajes de login, registro, ver y buscar perfiles.
  + Transporte de red seguro: tenemos pensado hacerlo con TLS.