Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

É um modulo dedicado a tratar a questão de segurança.

## Objetivos do Security

* Autenticação
  + Vai ser a forma de como o usuário vai se conectar ao serviço, seja por login e senha, token...
* Autorização
  + Vai ser o controle de acesso EX: usuario1, tem permissão de leitura, usuario2 tem permissão de escrita...
* Proteção contra principais ataques(CSRF, clickjacking, etc.)

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Em web Stateful tem as sessões o servidor guarda os dados do usuário em memória por um tempo, e ele sabe qual é cada usuário e o que ele está fazendo.

Agora já na aplicação API ela é Stateless, ou seja, ela não guarda o estado a cada requisição você deve ter seus dados.

Ou seja, você faz a requisição com seus dados o servidor te devolve e esquece quem é você, na próxima requisição você precisa se “apresentar novamente”

Lembrar que existe várias estratégias para você lidar com autenticação, mas uma dela que vamos utilizar vai ser o TOKEN (JWT – JSON Web Tokens)

Diagrama

Descrição gerada automaticamente

Imagina que o usuário digitou seu login e senha, após apertar em ENTRAR, ela vai disparar uma requisição para o API Rest Backend

La no Backend, vai esta o JSON com os dados que foram escritos pelo usuário

Agora o próximo passo e o Api Rest Backend que esta com os dados vai consultar la no SQL e ver se os dados é validos.

Os dados estão corretos? Então a API vai gerar um Token igual uma String.

Após gerar o token esse token vai ser devolvido para a aplicação que fez a requisição.

Lembrar que esse token tem que ser guardado na aplicação, existem técnicas para isso, porque é com esse token que vamos identificar que esse usuário esta logado.

Após isso caímos agora na autorização

Diagrama

Descrição gerada automaticamente

Agora ele vai preencher os dados do médico, vai clicar em salvar.

Vai ser mais ou menos a mesma pegada, vai ser levado um JSON para o Api Rest Backend e vai ter que ser incluído um cabeçalho que se chama Authorization: Bearer Token\_JWT

Esse cabeçalho vai ser levado o token que foi obtido no processo de login

Lembrar que o processo sempre vai ser assim, sempre vamos ter que levar o token que foi criado pelo usuário e todas as requisições vamos ter que validar esse token.

A API rest vai validar.

Existem diversas formas de se realizar o processo de autenticação e autorização em aplicações Web e APIs Rest, sendo que no curso utilizaremos **Tokens JWT**.

Você pode conferir as principais formas de autenticação lendo este artigo: [Tipos de autenticação](https://www.alura.com.br/artigos/tipos-de-autenticacao).