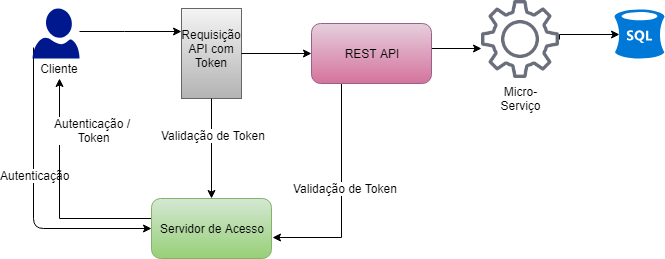
**Visão Segurança**

**1. Introdução**

O diagrama abaixo oferece detalhes sobre como é feita a segurança de dados da aplicação. Apresenta como é feita a autenticação do usuário e o acesso mediante a posse do token aos dados sensíveis presentes nos bancos de dados.

**2. Modelo**



**3. Elementos**

***3.1 Cliente***

É o usuário que está tentando acessar os dados da aplicação. Como o sistema é web a autenticação é requerida através de um browser. Se estiver tudo certo com a autenticação o usuário consegue um token com o qual consegue acesso aos dados.

***3.2 Servidor de Acesso***

Servidor responsável por guardar os dados de autenticação do usuário de forma criptografada. Ao receber um pedido de autenticação ele verifica a veracidade dos dados e fornece um token de acesso ao usuário, este token dá acesso às funcionalidades do sistema **de acordo com nível de privilégio do usuário**.

***3.3 REST API***

Todas as requisições feitas com a api REST necessita em seu cabeçalho do token de acesso para que o servidor possa validar essas requisições. Dessa forma ao receber o token no cabeçalho a primeira coisa a se verificar no servidor de acesso é se este token é válido. Caso seja o processo de requisição segue normalmente. Caso o token seja inválido ou tenha inspirado é retornado uma exceção de autorização e assim será necessário autenticar-se novamente.

***3.4 Micro Serviços***

Os micro serviços só serão acessados caso o token seja válido, para isso é imprescindível que seja feita a validação do mesmo com o server de autenticação. Uma vez validado o serviço segue seu fluxo.

**4. Embasamento**

Essa visão foi escolhida para atender ao ponto de vista de segurança e é importante pois ela dá detalhes de como é feita a autenticação do usuário e mostra como é feita a segurança dos dados presentes no servidor.