MÓDULO DE AUTENTICAÇÃO

1. OBJETIVO

O módulo de autenticação é uma aplicação web com base no json server, utilizando a framework express
e tendo como SGBD o MySQL, com a finalidade de gerenciar permissões (utilizando o json web token)
e proteger o sistema com senhas criptografadas utilizando SHA256, como sistema de segurança.

2. INFORMAÇÕES GERAIS

O sistema possui como componentes principais:

- *NodeJS*
- *MySQL*
- *Express*

Para a autenticação de usuários, foi utilizado o *JSON Web Token (JWT)* e a hash SHA 256 para gerar uma hash criada à partir da senha digitada pelo usuário, de forma que quando ela seja compatível com a senha presente no banco de dados.

JSON Web Token

Um *JWT* é um objeto contendo as informações do usuário codificados em uma *string*, sendo esta usada para autenticação do usuário e somente gerada uma única vez, pois quando é gerada novamente a assinatura digital muda.

No módulo de autenticação, o *jwt* está sendo utilizado quando o usuário é logado e guardado no *header* da página para futuras consultas de autenticação. No *json web token* está sendo utilizado o algoritmo HS256 no qual pede uma senha para codificar o *token*, e esta senha está sendo fornecida através de variáveis de ambiente, em um arquivo *.env* na raiz do projeto. Para poder decodificar o *token* é necessário a mesma senha que foi usada para codificar.

Dotenv

O *dotenv* armazena informações de conexão de banco de dados, usuário, senhas, etc. É gerado um arquivo de configuração *.env* na raiz do projeto, separado do código.

Middlewares

Middlewares são funções utilizadas no sistema para autenticação do usuário, para certificação de permissão, tais como visualizar conteúdo do portal ou se é um usuário administrador.

SHA 256:

Para o armazenamento e comparação de senhas, o *SHA256* foi a opção escolhida. O SHA(Secure Hash Algorithm) é um conjunto de operações matemáticas que geram uma hash de 256 bits, a qual será comparada com a senha cadastrada dentro do banco de dados, e então fornecerá o acesso ao usuário em caso de compatibilidade.

Autenticação:

Todas as autenticações são feitas através do JWT, que verifica se o token não foi alterado, comparando de acordo com a url de requisição, e por fim analisa as permissões do usuário.

```
auth: function(req, res, next){
        if ( global.userToken ) {
                try {
                        jwt.verify(global.userToken,  process.env.PASS_JWT, async (err, decode) => {
                                if(err){
                                        // dps mudar p render e passar mensagem de erro
                                        console.log('not enough privileges')
                                        res.redirect('/');
                                }
                                else {
                                        let user = await sql.findUserModuleByUserId(decode.id);
                                        if(user.length > 0){
                                                if(!req.originalUrl.toLowerCase().includes("middleware")){
                                                        var p = await user.find(el => {
                                                                return el.moduleLink.toLowerCase().includes(req.originalUrl.split('
                                                        })
                                                        if(!p){
                                                                console.log('not enough privileges')
                                                                res.redirect('/');
                                                        }
                                                        else{
                                                                return next();
                                                        }
                                                }else return next();
                                        }else{
                                                console.log('not enough privileges')
                                                res.redirect('/');
                                        }
                                }
                        });
                }catch(err){
                        res.redirect('/');
                }
        }else res.redirect('/');

},
```

Senha:

- Mínimo 6 caracteres
- Máximo 20 caracteres
- Pelo menos 1 letra maiúscula
- Pel

o

menos

1

número

Nome:

- Mínimo 3 caracteres
- Máximo 15 caracteres

Sobrenome:

- Mínimo 3 caracteres
- Máximo 20 caracteres

3. AUTORIZAÇÕES DO SISTEMA

Autorizações e permissões do sistema:

Usuário padrão

- Permissão para editar suas informações;
- Acesso somente a *view* "*login*" e às aplicações a ele designados pelo administrador.

Administrador

- Permissão para criar, editar e excluir todos os usuários do sistema;
- Acesso a todas as aplicações.