sexta-feira, 13 de maio de 2022 16:48

CONFIGURAÇÃO DA SEGURANÇA DO BANCO DE DADOS
(usar apenas quando o projeto já estiver finalizado ou nas etapas finais. Antes disso pode ser usado a configuração vista acima e depois modificar para essas configurações)

Alterar o código de segurança do banco de dados por um dos códigos abaixo:

Qualquer usuário pode ler e escrever os dados
 	
(método usado apenas para teste)
	rules_version = '2';
	service cloud.firestore {
	match /databases/{database}/documents {
	match /{document=**} {
	allow read, write: if //pode ler e escrever dados
	}
	}
	}

Qualquer usuário pode apenas ler os dados	rules_version = '2';
	service cloud.firestore {
	match /databases/{database}/documents {
	match /{document=**} {
	allow read: if true; //pode ler os dados
	allow write: if false; //não pode escrever dados
	}
	}
	}

Qualquer usuário pode apenas escrever dados	rules_version = '2';
	service cloud.firestore {
	match /databases/{database}/documents {
	match /{document=**} {
	allow read: if false; //não pode ler os dados
	allow write: if true; //pode escrever dados
	}
	}
	}

Apenas um usuário especifico pode ler e escrever dados	rules_version = '2';
	service cloud.firestore {
	match /databases/{database}/documents {

```
    match /{document=**} {
        allow read: if false; //não pode ler os dados
        allow write: if request.auth.uid == "colocar o id do usuário que pode modificar os dados";
    }
  }
}
```

Somente Usuários logados podem ler ou escrever dados

```
rules_version = '2';
service cloud.firestore {
  match /databases/{database}/documents {
    match /{document=**} {
        allow read,write: if request.auth !=null;
        //o usuário pode ler e escrever se o identificador do usuário for diferente de nulo
    }
  }
}
```

Somente os donos do conteúdo podem ler ou modificar:

```
service cloud.firestore {
  match /databases/{database}/documents {
    // Allow only authenticated content owners access
    match /some_collection/{userId}/{documents=**}{
        allow read,write:if request.auth !=null&&request.auth.uid =="colocar o id do dono do sistema";
    }
  }
}
```

Todos podem ler mas apenas os donos do conteúdo podem modificar:

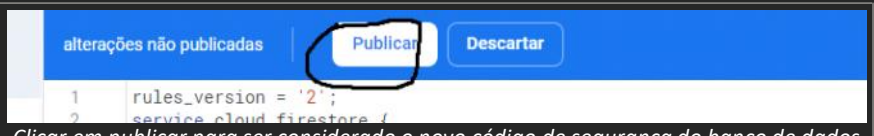
```
service cloud.firestore {
  match /databases/{database}/documents {
    // Allow public read access, but only content owners can write
    match /some_collection/{document}{
        allow read:iftrue
            allow create: if request.auth.uid ==request.resource.data.author_uid;
            allow update,delete: if request.auth.uid ==resource.data.author_uid;
    }
  }
}
```

Permissão baseada no papel do usuário:

```
service cloud.firestore {
  match /databases/{database}/documents {
    // For attribute-based access control, Check a boolean `admin` attribute
    allow write:ifget(/databases/$(database)/documents/users/$(request.auth.uid)).data.admin ==true;
    allow read:true;

    // Alterntatively, for role-based access, assign specific roles to users
    match /some_collection/{document}{
     allow read:ifget(/databases/$(database)/documents/users/$(request.auth.uid)).data.role
    =="Reader"
        allow write:ifget(/databases/$(database)/documents/users/$(request.auth.uid)).data.role
    =="Writer"
  }
  }
}
```

OBS: Existem outros métodos de segurança. Pesquisar na documentação do firebase



Clicar em publicar para ser considerado o novo código de segurança do banco de dados