Almacena y Sincroniza tus datos con Firebase

REGLAS DE USO DE FIRESTORE

1. **Restringir el acceso a la base de datos:**
   Puedes definir reglas para permitir o denegar el acceso a la base de datos en su totalidad. Por ejemplo, si deseas que solo los usuarios autenticados puedan acceder a Firestore, puedes establecer reglas como esta:

```
service cloud.firestore {
  match /databases/{database}/documents {
    // Solo permitir el acceso a usuarios autenticados
    allow read, write: if request.auth != null;
  }
}
```

2. **Controlar el acceso a colecciones y documentos específicos:**
   Puedes definir reglas para restringir el acceso a colecciones y documentos específicos en tu base de datos. Por ejemplo, puedes permitir que los usuarios solo lean y escriban sus propios documentos, pero no los de otros usuarios:

```
service cloud.firestore {
  match /databases/{database}/documents {
    // Solo permitir el acceso a documentos del usuario actual
    match /colección/{documentoId} {
      allow read, write: if request.auth.uid == resource.data.userId;
    }
  }
}
```

3. **Validar los datos:**
   Puedes utilizar las reglas de seguridad para validar los datos que se están escribiendo en Firestore. Por ejemplo, puedes asegurarte de que ciertos campos cumplan con ciertas condiciones antes de permitir que se guarden en la base de datos:

```
service cloud.firestore {
  match /databases/{database}/documents {
    match /colección/{documentoId} {
      // Validar que el campo "nombre" no esté vacío y tenga menos de 50 caracteres
      allow write: if request.resource.data.nombre != null
                   && request.resource.data.nombre is string
                   && request.resource.data.nombre.size() <= 50;
    }
  }
}
```

Las reglas de seguridad en función del tiempo te permiten controlar el acceso a los datos de Firebase Firestore basándote en el tiempo actual o en valores de fecha/hora almacenados en los documentos. Esto es útil para restringir el acceso a ciertos datos durante períodos específicos o para implementar lógica de expiración de documentos.

1. **Restringir el acceso basado en el tiempo actual:**
   Puedes limitar el acceso a una colección o documento en función del tiempo actual. Por ejemplo, puedes permitir el acceso solo durante ciertas horas del día:

```
service cloud.firestore {
  match /databases/{database}/documents {
    match /colección/{documentoId} {
      // Permitir el acceso solo de 9 a.m. a 5 p.m. UTC
      allow read, write: if request.time.hour() >= 9
                         && request.time.hour() < 17;
    }
  }
}
```

2. **Restringir el acceso basado en valores de fecha/hora almacenados:**
   Puedes utilizar valores de fecha/hora almacenados en los documentos para controlar el acceso. Por ejemplo, puedes permitir el acceso solo si la fecha actual está dentro de un rango específico definido en el documento:

```
service cloud.firestore {
  match /databases/{database}/documents {
    match /colección/{documentoId} {
      // Permitir el acceso solo si la fecha actual está dentro del rango especificado en el documento
      allow read, write: if request.time >= resource.data.fechaInicio
                         && request.time <= resource.data.fechaFin;
    }
  }
}
```

COMANDOS

```
firebase init

sudo npm install

// sudo npm install -g firebase-tools

eslint --fix index.js

firebase deploy
```