Ciclo 1 Universidad Don Bosco

Materia:

Diseño y Programación de Software Multiplataforma G01T

Nombre del trabajo:

FORO 2

Estudiante:

Guillermo Salvador Cartagena Mejia CM213015

Alan Anderson Vasquez Leiva VL221407

Kelly Abigail Vásquez Rodríguez VR220916

Julio César Posada Ramírez PR222058

Docente:

Ing. Alexander Alberto Sigüenza Campos

Link repositorio : https://github.com/Cartagena2001/DPS-FORO2

Link de video: https://drive.google.com/drive/folders/15ezCL_0k5HVZ6W-TIhyvaKnAhZfF3YYU?usp=sharing

Fecha de entrega: 04 de mayo de 2025

Contenido

Investigación sobre Opciones de Autenticación en Firebase para React Native

Objetivo de la investigación

El propósito de esta investigación es explorar y documentar en detalle las diferentes opciones de autenticación disponibles al utilizar Firebase en un proyecto desarrollado con React Native. Al proporcionar una descripción general completa que sirva como guía para tomar decisiones informadas al implementar sistemas de autenticación en aplicaciones móviles.

Opciones de Autenticación en Firebase

Firebase Authentication es una solución de autenticación completa que simplifica la incorporación de usuarios al proporcionar múltiples métodos seguros integrados y listos para usar. se muestra un desglose completo de las principales opciones que ofrece Firebase:

Correo electrónico y contraseña

describir: Permitir que los usuarios se registren y se autentiquen utilizando su dirección de correo electrónico y contraseña.

ventaja: Fácil de implementar.

Común y familiar para la mayoría de los usuarios.

Permite funciones como verificación de correo electrónico y restablecimiento de contraseña.

desventaja: Exigir a los usuarios que recuerden sus contraseñas.

Si se utilizan contraseñas débiles, aumenta el riesgo de intentos de acceso no autorizado.

Consideraciones:

Se recomienda implementar reglas de validación de contraseña y verificación de correo electrónico.

Es ideal para aplicaciones que desean un control total sobre el proceso de registro.

Google Sign-In

Descripción:
Permite a los usuarios iniciar sesión con sus cuentas de Google, integrando el sistema de OAuth 2.0 de forma sencilla.

Ventajas:

- Inicio de sesión rápido y sin necesidad de recordar contraseñas.
- Menor fricción para el usuario, especialmente en dispositivos Android.
- Amplio alcance, ya que muchas personas tienen cuentas de Google.

Desventajas:

- Requiere configuración en Firebase y en Google Cloud Console.
- No todos los usuarios tienen cuentas de Google (aunque son mayoría).

Consideraciones:

- Es una excelente opción para apps que buscan minimizar pasos de acceso y ofrecer una experiencia fluida.
- Es necesario configurar el webClientId correctamente para que funcione en Android e iOS.

Facebook Login

Descripción:
Permite autenticarse utilizando una cuenta de Facebook a través de su API oficial.

Ventajas:

- Popular en apps sociales y de entretenimiento.
- Permite acceso a datos básicos del perfil (nombre, correo, foto).

Desventajas:

- Requiere configuración en Facebook Developers y conexión con Firebase.
- Dependencia de una plataforma externa que puede tener cambios frecuentes.

Consideraciones:

- El diseño debe prever el uso de SDKs adicionales.
- La percepción del usuario puede variar dependiendo de la audiencia de la app (algunos públicos ya no utilizan Facebook activamente).

Apple

4. Apple Sign-In

Descripción:
Exclusivo para dispositivos Apple, permite iniciar sesión con una cuenta de Apple ID.

Ventajas:

- Recomendado (e incluso obligatorio) en apps iOS que ofrecen autenticación de terceros.
- Alta seguridad y privacidad (puede ocultar el correo del usuario).

Desventajas:

- Solo disponible en dispositivos iOS (iPhone, iPad).
- Requiere configuración en Apple Developer Console.

Consideraciones:

- Su implementación es obligatoria si se usan otros proveedores sociales en iOS.
- Proporciona una experiencia de usuario integrada y segura.

5. Autenticación Anónima

Descripción:
Permite a los usuarios acceder temporalmente a la app sin crear una cuenta.

Ventajas:

- Ideal para permitir el uso sin barreras iniciales (onboarding sin login).
- Puede combinarse con un proceso posterior de registro permanente.

Desventajas:

- No se asocian los datos a un usuario persistente si se borra la sesión.
- Requiere lógica adicional si se desea convertir la cuenta anónima en registrada.

Consideraciones:

- Útil para apps que quieren capturar usuarios antes de exigir registro (por ejemplo, probar funciones antes de registrarse).

6. Autenticación con Proveedor Personalizado (Custom Token)

Descripción:
Permite conectar Firebase Authentication con tu propio backend o sistemas de autenticación externos.

Ventajas:

- Máxima flexibilidad y control sobre la lógica de autenticación.
- Permite integrar sistemas corporativos o bases de usuarios existentes.

Desventajas:

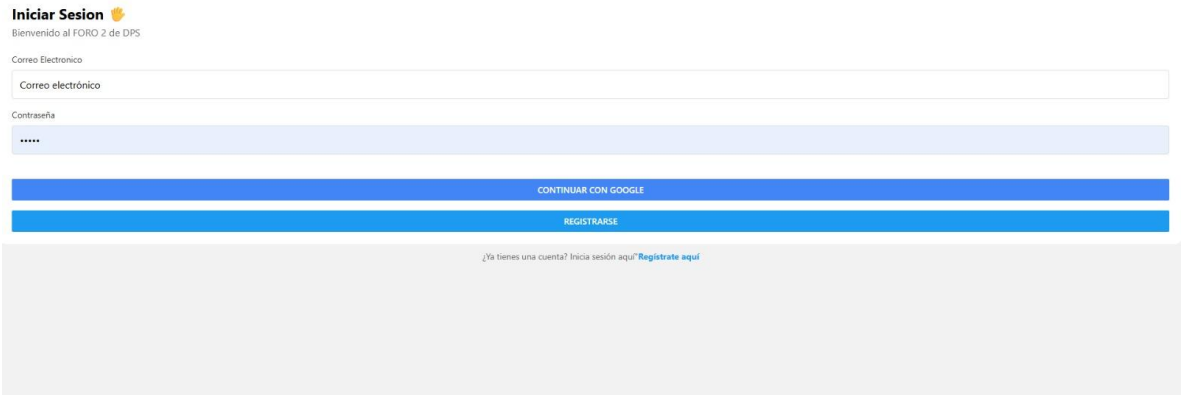
- Mayor complejidad técnica.
- Requiere infraestructura adicional para generar y validar tokens JWT.

Consideraciones:

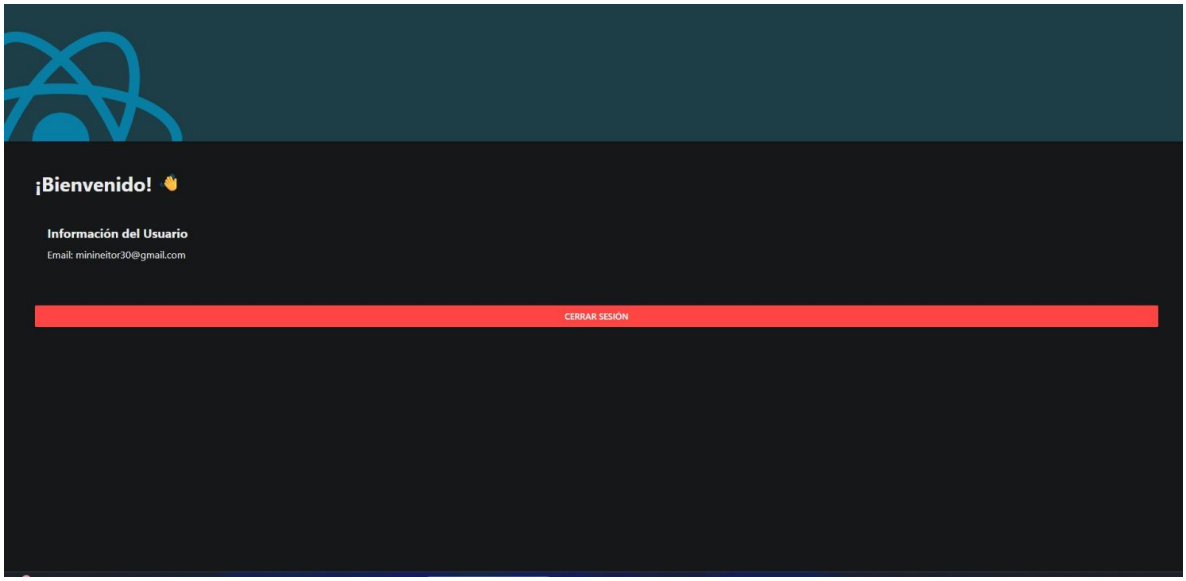
- Ideal para proyectos empresariales con necesidades específicas.
- El backend debe estar adecuadamente asegurado.

Aplicación realizada

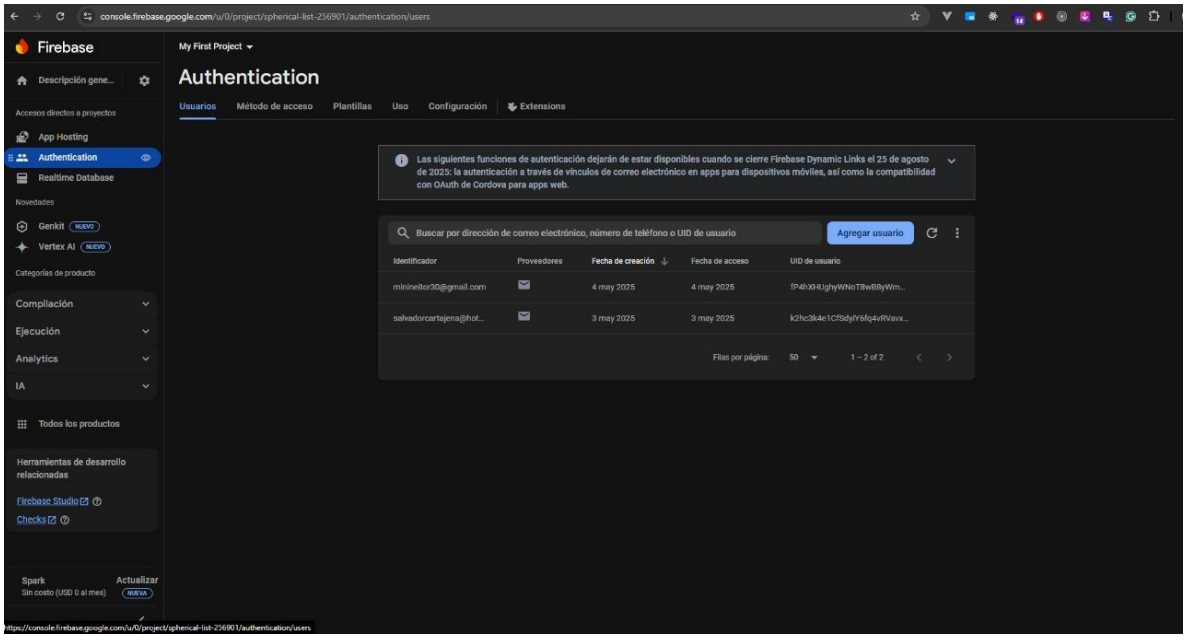
Pagina de inicio donde se podrán registrar y acceder a la aplicación



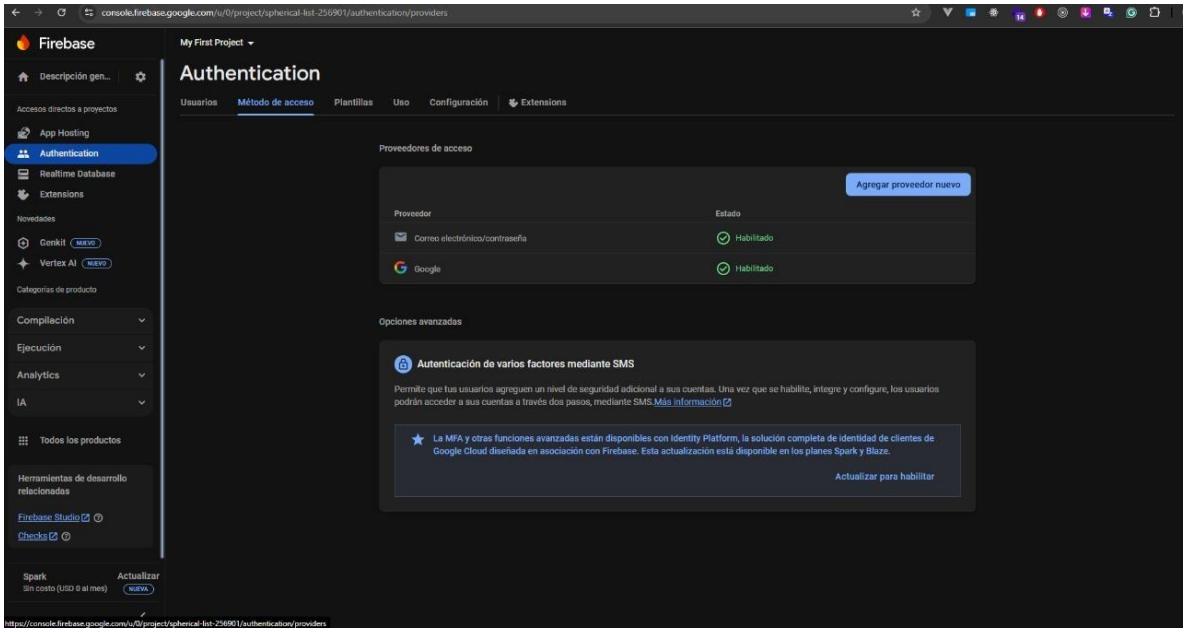
Pagina de Bienvenida



Registro de correos electrónicos



Registro de autenticación



Proyecto faro dos