**MESA DE AYUDA**

La mesa de ayuda fue desarrollada con una arquitectura modular, separando el frontend del backend. El frontend está construido con HTML, CSS y JavaScript, mientras que el backend utiliza Node.js con una base de datos MySQL. Esta estructura permite una fácil escalabilidad del proyecto y facilita futuras modificaciones, ya sea para optimizar el rendimiento o ampliar sus funcionalidades.

MESA-AYUDA/

├── backend/

│ ├── src/

│ │ ├── middlewares/

│ │ │ └── authMiddleware.js

│ │ ├── routes/

│ │ │ └── authRoutes.js

│ │ ├── services/

│ │ │ └── authService.js

│ │ ├── .env

│ │ ├── dbConfig.js

│ │ ├── package-lock.json

│ │ ├── package.json

│ │ └── server.js

└── frontend/

├── css/

│ ├── auth.css

│ └── panel-principal.css

├── js/

│ ├── auth.js

│ └── panel-principal.js

├── public/

└── views/

├── login.html

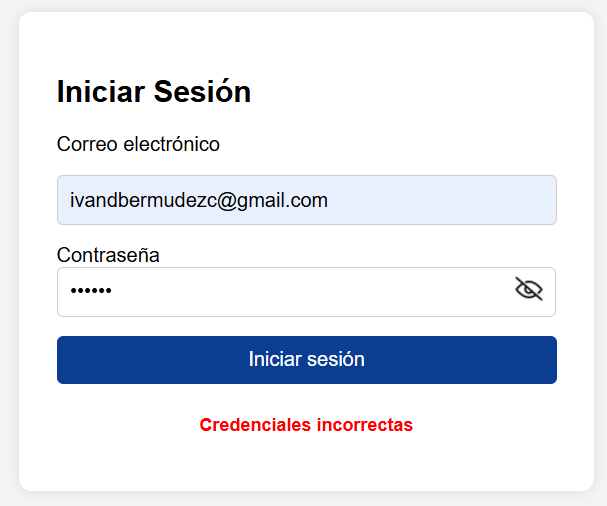
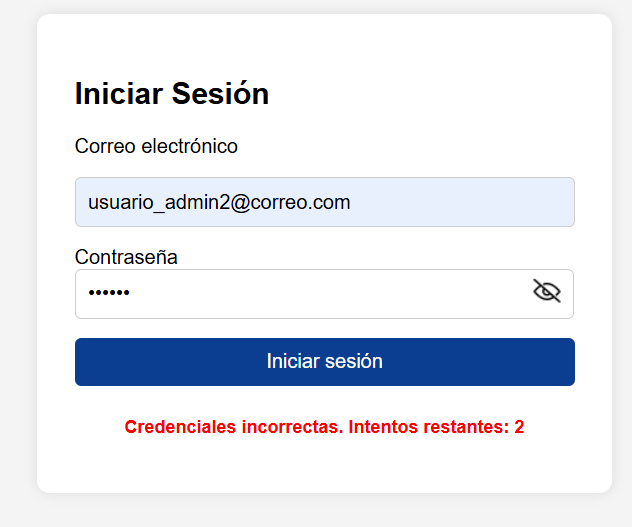
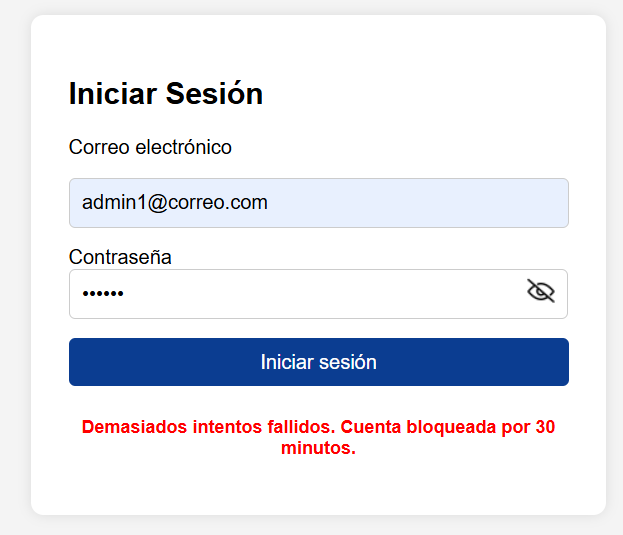
└── panel-principal.html

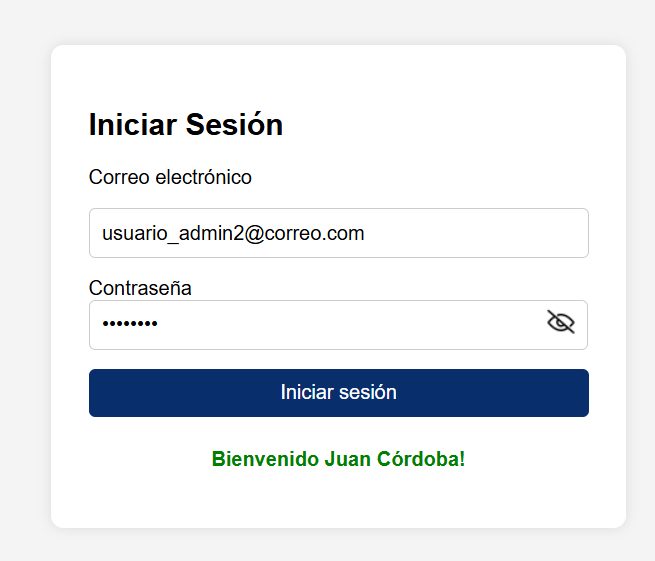
**Avance del Módulo de Autenticación - Mesa de Ayuda FOMAG**

Como parte del desarrollo inicial del sistema, se ha llevado a cabo la creación de la estructura base de datos, implementando las tablas fundamentales: roles, tipos de documento y usuarios. Estas tablas constituyen la base del módulo de autenticación, permitiendo un control estructurado del acceso al sistema.

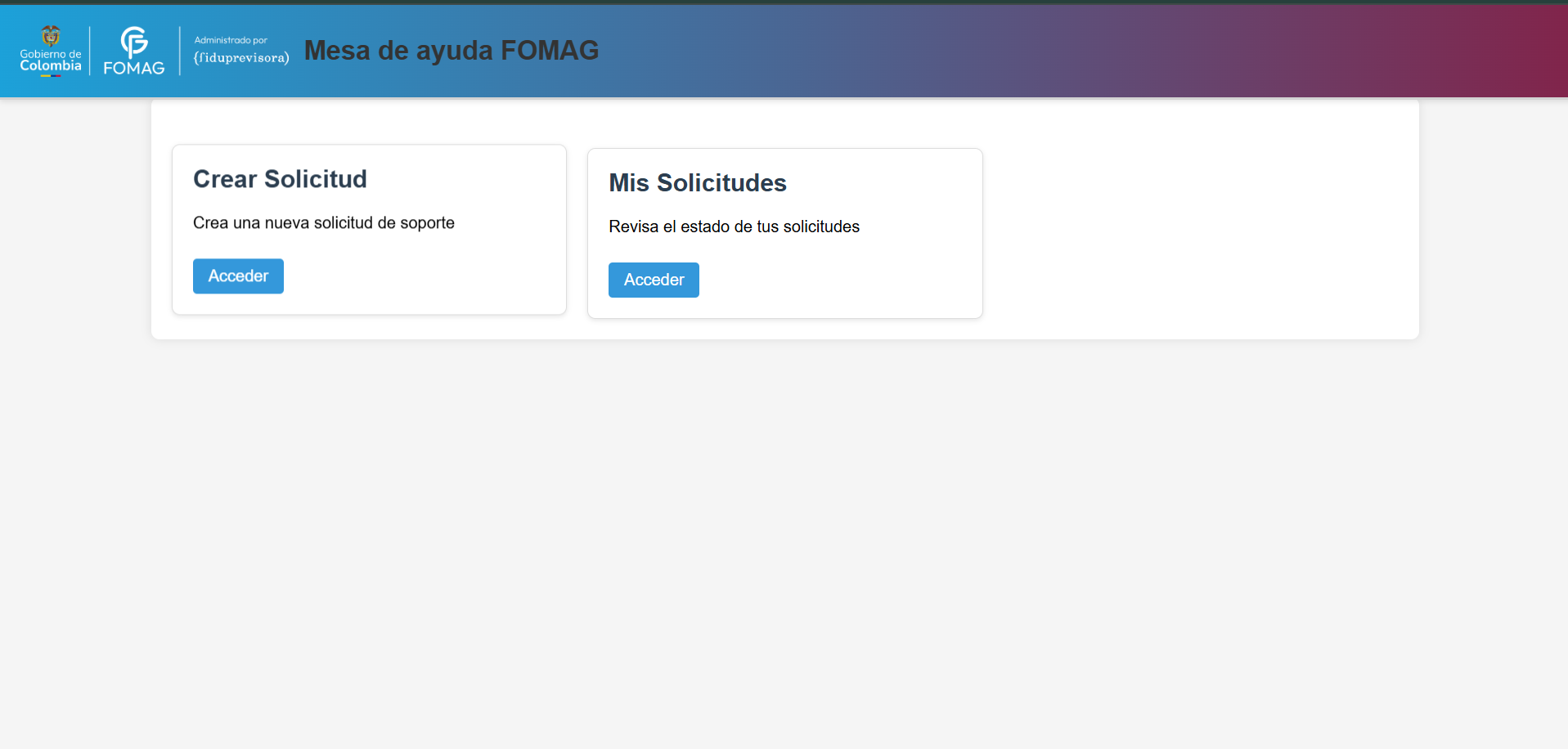
Implementación del proceso de inicio de sesión

Se diseñó e implementó un mecanismo de autenticación con enfoque en seguridad y control de acceso, con las siguientes características:

1. Validación de credenciales:
   * Si el usuario ingresa un correo electrónico no registrado, el sistema retorna un mensaje indicando que las credenciales son incorrectas, sin especificar si el error está en el correo o en la contraseña, como buena práctica de seguridad. 
2. Gestión de intentos fallidos:
   * Si el correo electrónico es válido pero la contraseña es incorrecta, el sistema activa un contador de intentos fallidos. 
   * Al alcanzar tres intentos fallidos consecutivos, la cuenta del usuario se bloquea automáticamente por un periodo de 30 minutos. 
3. Acceso según rol:
   * Si las credenciales son correctas, el usuario accede al panel de control.



* + Dependiendo del rol asignado (Administrador, Usuario Administrativo o Usuario General), se habilitan diferentes niveles de acceso y funcionalidades dentro del sistema.



Este esquema inicial sienta las bases para el desarrollo posterior del sistema de gestión de tickets, garantizando una autenticación segura y adaptable.