

# Integrantes

---

- Itzel Ramirez Flores
  - Angel de Jesus Torres Tejas
  - Samuel Armas Ocampo
  - Victor Manuel Morales Mejia
- 

## Caso de Uso 2: Iniciar Sesión

---

Campo	Descripción
Versión	1.0
Caso de Uso	Iniciar Sesión
Breve descripción	Caso de uso mediante el cual el sistema permite a un usuario registrado (miembro o administrador) autenticarse en la aplicación mediante sus credenciales (correo electrónico y contraseña) para acceder a las funcionalidades correspondientes a su rol.
Precondiciones	<ul style="list-style-type: none"><li>- El usuario debe tener una cuenta registrada en el sistema.</li><li>- La aplicación debe estar en funcionamiento.</li><li>- MongoDB debe estar disponible y conectado.</li><li>- El usuario debe estar en la pantalla de login correspondiente (miembro o administrador).</li></ul>
Postcondiciones	<ul style="list-style-type: none"><li>- El sistema ha autenticado al usuario exitosamente.</li><li>- Se crea una sesión de usuario activa.</li><li>- El usuario es redirigido al dashboard correspondiente a su rol.</li><li>- Se registra en bitácora la fecha, hora y usuario que inició sesión.</li></ul>
Flujos de eventos — Flujo principal	<ol style="list-style-type: none"><li>1) El usuario accede a la pantalla de bienvenida.</li><li>2) El usuario selecciona su tipo de login ("Iniciar sesión</li></ol>

	<p>como Miembro" o "Iniciar sesión como Administrador").</p> <p>3) El sistema presenta el formulario de login con los campos: correo electrónico y contraseña.</p> <p>4) El usuario ingresa su correo electrónico y contraseña.</p> <p>5) El usuario presiona el botón "Iniciar Sesión".</p> <p>6) El sistema valida que ambos campos estén completos.</p> <p>7) El sistema busca en la base de datos una cuenta con el correo electrónico proporcionado.</p> <p>8) El sistema verifica que la contraseña coincida con la almacenada.</p> <p>9) El sistema verifica que el rol del usuario coincida con el tipo de login seleccionado.</p> <p>10) El sistema crea una sesión de usuario.</p> <p>11) El sistema redirige al usuario al Dashboard correspondiente (Dashboard de Miembro o Dashboard de Administrador).</p>
Flujos alternos	<ul style="list-style-type: none"> <li>- <b>A1) Credenciales incorrectas:</b> Si el correo electrónico no existe en la base de datos o la contraseña no coincide, el sistema muestra un mensaje "Credenciales incorrectas. Por favor, verifica tu correo y contraseña" y permite al usuario intentar nuevamente.</li> <li>- <b>A2) Rol incorrecto:</b> Si el usuario intenta iniciar sesión como administrador pero su cuenta es de miembro (o viceversa), el sistema muestra un mensaje "Tipo de cuenta incorrecto. Por favor, selecciona el tipo de login correcto" y regresa a la pantalla de bienvenida.</li> <li>- <b>A3) Cancelación:</b> Si el usuario presiona el botón "Regresar", el sistema descarta los datos ingresados y regresa a la pantalla de bienvenida.</li> <li>- <b>A4) Registro de nuevo usuario:</b> Si el usuario no tiene cuenta, puede seleccionar la opción "Registrarse" y el sistema invoca el caso de uso CU-01 "Registro de Usuario".</li> </ul>
Flujos excepcionales	<ul style="list-style-type: none"> <li>- <b>E1) Error de conexión a la base de datos:</b> Si el sistema no puede conectarse a MongoDB al momento de validar las credenciales, muestra un mensaje "Error de conexión".</li> </ul>

	<p>Por favor, verifica que MongoDB esté ejecutándose" y no permite completar el inicio de sesión.</p> <ul style="list-style-type: none"> <li>- <b>E2) Campos vacíos:</b> Si el usuario intenta iniciar sesión sin completar ambos campos, el sistema muestra un mensaje "Por favor, completa todos los campos" y no procesa la solicitud.</li> <li>- <b>E3) Error al crear sesión:</b> Si ocurre un error técnico al crear la sesión de usuario, el sistema muestra un mensaje de error y sugiere intentar más tarde.</li> </ul>
Puntos de extensión	<ul style="list-style-type: none"> <li>- Recuperación de contraseña: puede agregarse una opción "¿Olvidaste tu contraseña?" que inicie un flujo de recuperación.</li> <li>- Límite de intentos: puede implementarse un bloqueo temporal de cuenta después de varios intentos fallidos.</li> <li>- Sesión persistente: opción "Recordarme" para mantener la sesión activa.</li> <li>- Autenticación de dos factores: puede agregarse un segundo nivel de verificación.</li> </ul>