**Historia de Usuario:**  
Como **usuario**, quiero **iniciar sesión en la aplicación** para **acceder a mis datos personales y funcionalidades privadas** según mi **nivel de permiso**.

**Criterios de Aceptación - Validación de Contraseña:**

1. La contraseña debe tener al menos **8 caracteres**.
2. La contraseña debe incluir al menos **una letra mayúscula**.
3. La contraseña debe incluir al menos **una letra minúscula**.
4. La contraseña debe contener al menos **un número**.
5. La contraseña debe tener al menos **un carácter especial** (por ejemplo: !@#$%^&\*()).
6. Si la contraseña no cumple alguna condición, debe mostrarse un **mensaje de error específico** indicando qué falta.
7. La validación debe realizarse **antes de enviar la solicitud al servidor** (validación en frontend).
8. La contraseña no debe ser visible por defecto (campo tipo **password**).

**Criterios de Aceptación - Acceso según Nivel de Permiso:**

1. Después de iniciar sesión, el usuario debe ser autenticado y su nivel de permiso determinado.
2. Se definirán **tres niveles de permisos**:
   * **Administrador:** acceso completo a todos los recursos y configuraciones.
   * **Editor:** acceso para crear y modificar recursos, pero sin acceso a configuraciones críticas.
   * **Lector:** acceso únicamente a visualizar recursos, sin posibilidad de modificación.
3. Los usuarios solo podrán acceder a los recursos que su nivel de permiso les permita:
   * Acceso a rutas protegidas según su rol.
   * Las opciones no autorizadas deben estar ocultas o deshabilitadas en la interfaz.
4. Si un usuario intenta acceder a un recurso sin permiso, debe ser redirigido a una página de **"Acceso denegado"** o recibir un **mensaje claro**.
5. Los permisos deben validarse **tanto en frontend como en backend**.