Tabla 1: Doctores

Campo	Tipo de dato	Descripción
id	primary key (auto incremental)	Identificador único de cada usuario (doctor).
nombre	str	Nombre completo del doctor.
email	str	Correo electrónico del doctor (usado para login).
contraseña	str (hashed)	Contraseña encriptada del doctor.

Tabla 2: Imágenes DICOM

Campo	Tipo de dato	Descripción
id	primary key (auto incremental)	Identificador único de cada imagen DICOM.
archivo	File Path	Ruta del archivo DICOM almacenado.
patien_id	Clave foránea	Relación con la tabla de pacientes.
subida_por	Clave foránea	Relación con la tabla de usuarios (doctor que subió la imagen).
doctores_permitidos	Clave foránea	Relación con la tabla doctores (aquellos que pueden ver la imagen).
fecha_subida*	DateTime	Fecha en la que se subió la imagen.

* Evaluar si es necesario, ya que no sabemos al momento de crear la tabla si es relevante la info.

Tabla 3: Pacientes

Campo	Tipo de dato	Descripción
id	primary key (Auto Increment)	Identificador único de cada paciente.
nombre	String (255)	Nombre completo del paciente.
fecha_nacimiento	Date	Fecha de nacimiento del paciente.
doctor_id	Clave foránea	Relación con el doctor (de la tabla de usuarios)

Tabla 4: Carpetas

Campo	Tipo de dato	Descripción
id	Primary key (auto incremental)	Identificador único de cada carpeta.
nombre	str	Nombre de la carpeta.
doctor_id	clave foránea	Relación con el doctor (de la tabla de usuarios).
paciente_id	clave foránea	Relación con la tabla de pacientes.

Tabla 5: Logs de Acceso

Campo	Tipo de dato	Descripción
id	primary key	Identificador único del log.
usuario_id	clave foránea	Relación con la tabla de usuarios (doctores).
accion	str	Acción realizada (por ejemplo, "subió una imagen", "inició sesión").
fecha_accion	date time	Fecha y hora en que se realizó la acción.

Tabla 6: Sesiones

Campo	Tipo de dato	Descripción
id	primary key	Identificador único de la sesión.
usuario_id	clave foránea	Relación con la tabla de usuarios.
token_session	str	Token de sesión único.
inicio_session	date time	Fecha y hora en la que comenzó la sesión.
expire_session	date time	Fecha y hora en la que expira la sesión.

Endpoints

1. **Login:** Probar que el sistema permita acceder correctamente a la aplicación y que las credenciales sean válidas.
   - Test para validar un login exitoso.
   - Test para evitar que se acceda con contraseñas incorrectas.
2. **Carga de imágenes DICOM:** Asegurarse de que la subida de imágenes funciona correctamente.
   - Test para subir un archivo DICOM válido.
   - Test para rechazar un archivo con formato no válido.
3. **Búsqueda de imágenes:** Probar que las imágenes se pueden buscar por ID de paciente.
   - Test para buscar imágenes de un paciente específico.
   - Test para comprobar que no se devuelvan resultados incorrectos.
4. **Carpetas:** Probar que las carpetas se pueden crear y que se pueden almacenar imágenes dentro.
   - Test para crear carpetas asociadas a pacientes.
   - Test para verificar que las imágenes están correctamente organizadas dentro de las carpetas.

* Endpoints en rojo son los a testear en esta entrega

Tablas con inputs, salida esperada y contexto de ejecución

1. Login

Input	Salida Esperada	Contexto de ejecución
Email y contraseña correctos	Redirección a la página principal del sistema después del login.	El usuario ingresa su email y contraseña correctos en el formulario de inicio de sesión.
Email correcto, contraseña incorrecta	Mostrar mensaje de error: "Credenciales incorrectas"	El usuario ingresa su email correcto pero una contraseña incorrecta y envía el formulario.
Email no registrado	Mostrar mensaje de error: "Usuario no encontrado"	El usuario ingresa un email que no está registrado en el sistema.
Email vacío y contraseña vacía	Mostrar mensaje de error: "El campo email y contraseña son obligatorios".	El usuario envía el formulario sin completar los campos requeridos.
Contraseña vacía	Mostrar mensaje de error: "La contraseña es obligatoria".	El usuario deja el campo de la contraseña vacío y envía el formulario.
Email en formato incorrecto	Mostrar mensaje de error: "Formato de email inválido".	El usuario ingresa un email que no cumple con el formato de email válido (por ejemplo, sin "@" o dominio incorrecto).

Explicación de los Casos:

- Caso de éxito (Email y contraseña correctos): El sistema debe redirigir al usuario a la página principal, o al dashboard, después de iniciar sesión con las credenciales correctas. Se verifican tanto el email como la contraseña contra la base de datos.
- Casos de error (credenciales incorrectas o faltantes): El sistema debe manejar de manera adecuada los errores de autenticación, como credenciales incorrectas, campos vacíos, o un email con formato incorrecto. En estos casos, se muestra un mensaje de error apropiado sin permitir el acceso al sistema.