Database Documentation

Versión:	3.0
Date:	15/11/2023
Business:	Ing. Juan Carlos Monteros Ing. Francisco Orozco De La Hoz Lic. Leandro Dikenstein
Sponsor Organization:	UNGS
Authors:	Benitez, Micaela Benitez, Yamila Clauser, Nahuel Gómez, Federico Perez, Giannina Prieto, Lucas Torrico, Franco
Target Release:	Noviembre 2023

ÍNDICE

1. SCOPE DE LA BASE DE DATOS

Se implementó una base de datos relacional en PostgreSQL para gestionar datos relacionados con modelos de machine learning, diagnósticos médicos, usuarios del sistema, establecimientos médicos e imágenes utilizadas para realizar diagnósticos.

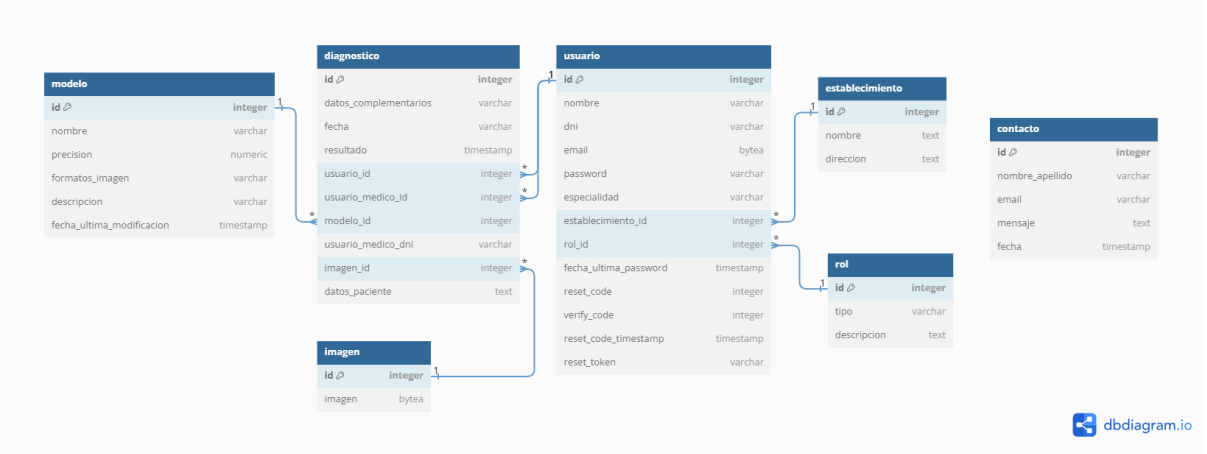
El objetivo principal de esta documentación es servir como una guía completa para desarrolladores, administradores de bases de datos y partes interesadas involucradas en la aplicación de análisis de imágenes médicas. Está diseñado para dilucidar la estructura, las funcionalidades y el flujo de datos dentro de la base de datos, fomentando una comprensión unificada de su arquitectura y operaciones.

1.1. Descripción general de la base de datos:

- Nombre BD: Pruebas
- Propósito: PruebasBD será una base de datos relacional diseñada para almacenar datos que posteriormente van a ser levantados con API's. Su propósito principal será para que tanto el equipo de front como los equipos de los modelos puedan utilizar los datos.
- Alcance: La BD contendrá datos de los médicos y usuarios, imágenes médicas de prueba, información del historial de todo lo realizado y el feedback de los médicos.
- Partes claves interesadas: Equipo de front y los equipos de los modelos.
- Meta: PruebasDB se basa en la conexión de todos los equipos y el almacenamiento de datos de estos.
- Fuente de los datos: Ingresada por los usuarios tanto como los equipos.
- Frecuencia de las actualizaciones: La BD se actualiza en tiempo real a medida que los clientes interactúan con nuestra plataforma.
- Accesibilidad: El acceso a PruebasBD se controla a través de roles de usuario, con diferentes niveles de acceso dependiendo del equipo.
- Dependencias: La base de datos se basará en los datos recibidos tanto en la plataforma de ingreso de datos diseñada como en los datos recibidos por los modelos.
- Arquitectura de alto nivel: La base de datos usa PostgreSQL como el DBMS y está alojado a través de Ngrok. Estará integrado con el front y los modelos a través de API.

.

2. DIAGRAMA ENTIDAD-RELACIÓN



3. ESTRUCTURA

Detalle y desglose de las tablas ubicadas en la base de datos con sus respectivas PK y FK y los tipos de datos que reciben.

3.1. Tabla Modelo

Almacena información sobre los modelos de diagnóstico que se utilizan en el sistema.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del modelo
nombre	character varying (255)		Nombre del modelo
precisión	numeric		Precisión del modelo
formatos de imagen	character varying (255)		Formatos de imagen que soporta el modelo

descripción	text		Descripción del modelo
fecha_última_modificación	timestamp without time zone		Fecha de la última modificación del modelo

3.2. Tabla Diagnóstico

Almacena información sobre los diagnósticos realizados por los modelos.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del diagnóstico
datos complementarios	text		Datos complementarios necesarios para obtener un diagnostico mas preciso
fecha	timestamp without time zone		Fecha en la que se realizó el diagnóstico
resultado	text		Predicción del modelo
usuario_id	integer	FK, NOT NULL	Usuario que realizo el diagnostico
usuario_medico_id	integer	FK	Medico que realizo el diagnostico
modelo_id	integer	FK	Modelo utilizado para realizar el diagnóstico
usuario_medico_dni	character varying (55)		Dni del medico que realizo el diagnostico
imagen_id	integer	FK	Identificador único de la imagen que se utilizó para realizar el

			diagnóstico
datos_paciente	text		Datos del paciente

3.3. Tabla Usuario

Almacena información sobre los usuarios del sistema.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del usuario
nombre	character varying (255)		Nombre del usuario
dni	character varying (255)		Dni del usuario
email	bytea		Email del usuario
password	character varying (255)		Contraseña del usuario
especialidad	character varying (255)		Especialidad del usuario
establecimiento_id	integer	FK	Establecimiento donde trabaja el usuario
rol_id	character varying (55)	FK	Rol del usuario
fecha_ultima_password	integer		Fecha en la que se creó la contraseña
reset_code	integer		Código para poder resetear la contraseña
verify_code	integer		Código para realizar la verificación doble
reset_code_timestamp	timestamp without time zone		Fecha en la que se solicitó el código

reset_token	character varying		Token para resetear contraseña

3.4. Tabla Establecimiento

Almacena información sobre los establecimientos médicos que utilizan el sistema.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del establecimiento
nombre	text		Nombre del establecimiento
dirección	text		Dirección del establecimiento

3.5. Tabla Rol

Almacena información sobre los roles que pueden tener los usuarios del sistema.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del rol
tipo	character varying (50)		Nombre del rol
descripción	text		Descripción del rol

3.6. Tabla Imagen

Almacena información sobre las imágenes que se utilizan para realizar los diagnósticos.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único de la imagen
imagen	bytea		Datos de la imagen en base64

3.7. Tabla Contacto

Almacena información sobre las solicitudes de contacto de los usuarios.

Campo	Tipo de dato	Restricción	Descripción
id	Integer, auto incrementable	PK, NOT NULL	Identificador único del usuario
nombre_apellido	character varying (255)		Nombre y apellido del usuario
email	character varying (255)		Email del usuario
mensaje	text		Mensaje
fecha	timestamp without time zone		Fecha en la que se envió el mensaje

4. FLUJO DE DATOS

El flujo de datos implica detallar cómo la información se mueve a través del sistema, desde sus puntos de entrada hasta diversas transformaciones y salidas finales.

4.1. Flujo de datos para las predicciones

4.1.1. **Flujo de datos para la predicción del diagnóstico cerebral**:

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica que contiene datos relacionados con el cerebro.
Consultas Médicas:
Pérdida visual (perdida_visual): El usuario proporciona un valor booleano que indica la pérdida visual.
Debilidad focal (debilidad_focal): Valor booleano que indica debilidad focal.
Convulsiones: Valor booleano que indica la presencia de convulsiones.
Detalles médicos y de usuario:
ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.
Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Procesamiento y predicción:

Preprocesamiento de datos: el archivo de imagen recibido se envía al modelo relacionado con el de cerebro para poder ser analizada junto con los datos

Cifrado de imagen: el archivo de imagen recibido se cifra en formato bytea.

Integración de consultas: las consultas médicas y los detalles del usuario se integran en el modelo de predicción para proporcionar información contextual para el diagnóstico.

Predicción de diagnóstico cerebral: los datos de imágenes preprocesadas, junto con los datos médicos integrados y los detalles del usuario, se introducen en el algoritmo o modelo de diagnóstico para afecciones relacionadas con el cerebro (p. ej., tumores, anomalías).

Salida de diagnóstico:

Resultado de predicción: el algoritmo genera un resultado de diagnóstico basado en los datos de entrada, lo que potencialmente indica un diagnóstico relacionado con el cerebro (p. ej., condiciones potenciales).
Respuesta al usuario/médico: el resultado del diagnóstico se presenta o se transmite al usuario y/o al médico que inició el proceso de diagnóstico.

4.1.2. Flujo de datos para análisis de corazón

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica relacionado con el análisis del corazón.
Consultas médicas adicionales:
Palpitaciones (palpitaciones): Valor booleano que indica palpitaciones.
Dolor en la parte superior izquierda del pecho (dolor_superior_izquierdo): Valor booleano que indica dolor en el pecho que se irradia a la parte superior izquierda del cuerpo.
Dificultad para respirar (disnea): Valor booleano que indica dificultad para respirar.
Detalles médicos y de usuario:
ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.

Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Manejo y cifrado de imágenes:

Cifrado de imagen: el archivo de imagen relacionado con el corazón recibido se cifra en formato bytea.
Almacenamiento en una tabla separada: los datos de la imagen cifrada se almacenan en una tabla dedicada con una identificación asociada.
Referencia en la tabla de diagnóstico: la tabla de diagnóstico incluye una referencia (clave externa) al ID de imagen correspondiente almacenado en la tabla imagen_analisis.

Integración y Transmisión al Modelo:

Integración de datos: combina todas las consultas de los usuarios, los detalles del usuario y la referencia de la imagen cifrada en un formato de datos estructurado para su transmisión.
Modelo para análisis cardíaco: los datos combinados se envían al "Modelo" para análisis cardíaco, que incluye la imagen cifrada y todos los detalles de consultas médicas y de usuarios asociados.

Salida de diagnóstico:
Resultado de predicción: el modelo genera un resultado de diagnóstico basado en los datos integrados, proporcionando información relacionada con el análisis del corazón.

4.1.3. Flujo de datos para análisis de muñeca

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica relacionado con el análisis de la muñeca.
Consultas médicas adicionales para muñeca:
Dolor por limitación funcional (dolor_con_limitacion): Valor booleano que indica dolor con limitación funcional.

Presencia de Edema (edema): Valor booleano que indica la presencia de edema.
Indicación de Deformidad (deformity): Valor booleano que indica la presencia de deformidad.
Detalles médicos y de usuario:
ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.
Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Manejo y cifrado de imágenes:

Cifrado de imagen: cifra el archivo de imagen relacionado con la muñeca recibido en formato bytea.
Almacenamiento en una tabla separada: almacena los datos de la imagen cifrada en una tabla dedicada con una identificación asociada.
Referencia en la tabla de diagnóstico: la tabla de diagnóstico incluye una referencia a la ID de imagen correspondiente almacenada en la tabla imagen_analisis.

Integración y Transmisión al Modelo:

Integración de datos: combina todas las consultas de los usuarios, los detalles del usuario y la referencia de la imagen cifrada en un formato de datos estructurado para su transmisión.
Modelo para análisis de muñeca: Transmita los datos combinados al "Modelo" diseñado específicamente para el análisis de muñeca, incluida la imagen cifrada y todos los detalles de consultas médicas y de usuario asociados.

Salida de diagnóstico:
Resultado de predicción: el modelo genera conocimientos de diagnóstico relacionados con el análisis de la muñeca basándose en los datos integrados, proporcionando información sobre posibles condiciones o problemas relacionados con la muñeca.

4.1.4. **Flujo de datos para análisis pulmonar**:

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica relacionado con el análisis pulmonar.
Consultas médicas adicionales para los pulmones:
Puntada lateral (puntada_lateral): Valor booleano que indica costura lateral.
Presencia de Fiebre (fiebre): Valor booleano que indica la presencia de fiebre.
Dificultad Respiratoria (dificultad_respiratoria): Valor booleano que indica dificultad respiratoria.
Detalles médicos y de usuario:
ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.
Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Manejo y cifrado de imágenes:
Cifrado de imagen: cifre el archivo de imagen relacionado con los pulmones recibido en formato bytea.
Almacenamiento en una tabla separada: almacena los datos de la imagen cifrada en una tabla dedicada con una identificación asociada.
Referencia en la tabla de diagnóstico: la tabla de diagnóstico incluye una referencia (clave externa) a la ID de imagen correspondiente almacenada en la tabla imagen_analisis.

Integración y Transmisión al Modelo:

Integración de datos: combine todas las consultas de los usuarios, los detalles del usuario y la referencia de la imagen cifrada en un formato de datos estructurado para su transmisión.

Modelo para análisis pulmonar: Transmita los datos combinados al "Modelo" diseñado específicamente para el análisis pulmonar, incluida la imagen cifrada y todos los detalles de consultas médicas y de usuario asociados para afecciones relacionadas con los pulmones.

Salida de diagnóstico:
Resultado de predicción: el modelo genera conocimientos de diagnóstico relacionados con el análisis pulmonar en función de los datos integrados, proporcionando información sobre posibles afecciones o problemas relacionados con los pulmones.

4.1.5. **Flujo de datos para el análisis de riñón**:

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica relacionado con el análisis del riñón.
Consultas médicas adicionales para riñones:
Hematuria (hermaturia): Valor booleano que indica la presencia de sangre en la orina (hematuria).
Dolor Lumbar (dolor_lumbar): Valor booleano que indica dolor lumbar o lumbar.
Dolor Abdominal (dolor_abdominal): Valor booleano que indica dolor abdominal.
Presencia de Fiebre (fiebre): Valor booleano que indica la presencia de fiebre.
Pérdida de Peso (perdida_peso): Valor booleano que indica pérdida de peso.
Detalles médicos y de usuario:
ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.
Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Manejo y cifrado de imágenes:

Cifrado de imagen: cifre el archivo de imagen relacionado con el riñón recibido en formato bytea.
Almacenamiento en una tabla separada: almacene los datos de la imagen cifrada en una tabla dedicada con una identificación asociada.
Referencia en la tabla de diagnóstico: la tabla de diagnóstico incluye una referencia (clave externa) a la ID de imagen correspondiente almacenada en la tabla imagen_analisis.

Integración y Transmisión al Modelo:
Integración de datos: combina todas las consultas de los usuarios, los detalles del usuario y la referencia de la imagen cifrada en un formato de datos estructurado para su transmisión.
Modelo para análisis de riñón: Transmita los datos combinados al "Modelo" diseñado específicamente para el análisis de riñón, incluida la imagen cifrada y todos los detalles de consultas médicas y de usuario asociados para afecciones relacionadas con el riñón.

Salida de diagnóstico:
Resultado de predicción: el modelo genera conocimientos de diagnóstico relacionados con el análisis de los riñones basándose en los datos integrados, proporcionando información sobre posibles afecciones o problemas relacionados con los riñones.

4.1.6. Flujo de datos para análisis de rodilla

Entrada de datos:

Archivo de imagen: el usuario carga un archivo de imagen médica relacionado con el análisis de la rodilla.
Consultas médicas adicionales para rodillas:
Sensación de inestabilidad (sensacion_inestabilidad): Valor booleano que indica sensación de inestabilidad en la rodilla.
Test de Cajón Anterior Positivo (CA_positiva): Valor booleano que indica un resultado positivo en el test “Cajón Anterior”.
Impotencia Funcional (impotencia_funcional): Valor booleano que indica impotencia funcional en la rodilla.
Detalles médicos y de usuario:

ID de usuario (id_usuario): Valor entero que identifica al usuario.
Identificación Nacional del Médico (dni_medico): Valor de cadena que identifica al médico.
Fecha de Nacimiento (fecha_nacimiento): Valor de cadena que representa la fecha de nacimiento del usuario.
Peso (peso): Valor entero que representa el peso del usuario.
Altura: Valor entero que representa la altura del usuario.
Género (sexo): Valor de cadena que indica el género del usuario.

Manejo y cifrado de imágenes:

Cifrado de imagen: cifre el archivo de imagen relacionado con el riñón recibido en formato bytea.
Almacenamiento en una tabla separada: almacene los datos del archivo cifrado/procesado en una tabla dedicada con una identificación asociada.
Referencia en la tabla de diagnóstico: la tabla de diagnóstico incluye una referencia (clave externa) al ID del archivo correspondiente almacenado en la tabla imagen_analisis.

Integración y Transmisión al Modelo:

Integración de datos: combine todas las consultas de los usuarios, los detalles del usuario y la referencia del archivo cifrado/procesado en un formato de datos estructurado para su transmisión.
Modelo para análisis de rodilla: Transmita los datos combinados al "Modelo" diseñado específicamente para el análisis de rodilla, incluido el archivo cifrado/procesado y todos los detalles de consultas médicas y de usuarios asociados para afecciones relacionadas con la rodilla.

Salida de diagnóstico:

Resultado de predicción: el modelo genera conocimientos de diagnóstico relacionados con el análisis de la rodilla en función de los datos integrados,

proporcionando información sobre posibles afecciones o problemas relacionados con la rodilla.

4.1.7. Flujo de datos para eliminar el diagnóstico:

Solicitud de eliminación recibida:
El sistema recibe una solicitud de eliminación de un registro de diagnóstico específico identificado por su ID (diagnostico_id).

Identificación de Imagen Asociada:

Utilizando el ID de diagnóstico recibido (diagnostico_id), el sistema identifica la imagen asociada, si la hay, vinculada a este registro de diagnóstico en la base de datos.

Proceso de eliminación de imágenes:

Si se encuentra una imagen asociada:
El sistema recupera la referencia a la imagen (por ejemplo, ImageID) vinculada al registro de diagnóstico utilizando la ID de diagnóstico.
El sistema inicia un proceso de eliminación del registro de imagen asociado de la tabla de imágenes correspondiente en función de la referencia recuperada (imagen_id).

Eliminación de diagnóstico:

Posteriormente, el sistema procede a eliminar el registro de diagnóstico especificado identificado por el ID de diagnóstico proporcionado (diagnostico_id) de la tabla Diagnóstico.

4.1.8. Flujo de datos para recuperar diagnósticos basados en la ID de usuario y la ID de función:

Solicitud recibida:

El sistema recibe una solicitud para recuperar diagnósticos basados en un ID de usuario y un ID de rol específicos.

Verificación de usuarios y roles:

El sistema valida el ID de usuario y el ID de rol proporcionados para garantizar que existan y sean válidos dentro de la administración de usuarios y roles del sistema.
Ejecución de consultas:

Utilizando el ID de usuario y el ID de rol validados, el sistema ejecuta una consulta en la base de datos, específicamente dirigida a la tabla de Diagnóstico.
Recuperación de diagnósticos:

La consulta recupera todos los registros de diagnóstico que coinciden con los criterios de ID de usuario y de ID de rol proporcionados de la tabla Diagnóstico.
Generación de respuesta:

Los registros de diagnóstico recuperados se compilan en un formato de respuesta adecuado para la transmisión.

Transmisión de Diagnósticos:

El sistema transmite los registros de diagnóstico compilados como respuesta al solicitante, proporcionando los diagnósticos relevantes asociados con el usuario y el ID de rol especificados.

4.1.9. Flujo de datos para recuperar un registro de diagnóstico específico según la ID de función y la ID de diagnóstico:

Solicitud recibida:

El sistema recibe una solicitud para recuperar un registro de diagnóstico específico basado en una ID del rol y una ID de diagnóstico única.

Verificación de ID de rol:

El sistema valida el ID de rol proporcionado para garantizar que sea auténtico y esté autorizado para acceder a los registros de diagnóstico.
Validación de identificación de diagnóstico:

El sistema verifica la identificación de diagnóstico proporcionada para garantizar que exista dentro de la base de datos de registros de diagnóstico del sistema.
Ejecución de consultas:

Utilizando el ID de función validado y el ID de diagnóstico, el sistema ejecuta una consulta en la base de datos, específicamente dirigida a la tabla de Diagnóstico.

Recuperación de Registro de Diagnóstico Específico:

La consulta recupera el registro de diagnóstico específico que coincide con el ID de diagnóstico proporcionado y al que puede acceder el ID de rol autorizado.
Generación de respuesta:

El registro de diagnóstico recuperado se formatea en un formato de respuesta apropiado.
Transmisión de Registro de Diagnóstico:

El sistema envía el registro de diagnóstico compilado como respuesta al solicitante, proporcionando los detalles del registro de diagnóstico específico.

4.2. Flujo de datos para el control y acciones de usuarios.

4.2.1. Flujo de datos de registro de usuario:

Recopilación de datos de entrada:

Nombre (nombre): Nombre del usuario.
Apellido (apellido): Apellido del usuario.
DNI (dni): Número de identificación del usuario.
Correo electrónico (email): Dirección de correo electrónico del usuario (cifrada por seguridad).
Contraseña (contraseña): Contraseña del usuario (con hash por seguridad).
ID de rol (rol_id): Identificador del rol del usuario.
ID de establecimiento (establecimiento_id): Identificador del establecimiento (si corresponde).
Especialización: Especialización del usuario (si corresponde).
Procesamiento de datos:

Cifrado (correo electrónico): cifre la dirección de correo electrónico proporcionada para su almacenamiento y procesamiento seguros dentro del sistema.
Hashing (contraseña): aplica hash a la contraseña proporcionada para un almacenamiento y verificación seguros sin almacenar la contraseña real.
Validación y Sanitización:

Valida el formato y la exactitud de los datos de entrada (por ejemplo, formato de correo electrónico, seguridad de la contraseña).
Desinfecta los datos para evitar posibles amenazas a la seguridad
Proceso de registro:

Ejecuta una consulta de base de datos o una llamada API para almacenar los detalles de registro del usuario en la base de datos del sistema.
Almacene el correo electrónico cifrado y la contraseña hash junto con otros detalles del usuario en la tabla de la base de datos de usuarios.
Manejo de respuestas:

Generar una respuesta indicando el éxito o fracaso del proceso de registro.
Devuelve un mensaje apropiado al usuario tras el registro exitoso o le solicita que vuelva a intentarlo en caso de cualquier falla.
Medidas de seguridad:
Cifrado (correo electrónico): utiliza técnicas de cifrado para proteger los datos de correo electrónico del usuario durante el almacenamiento y la transmisión.
Hashing (contraseña): emplea algoritmos de hash para proteger las contraseñas de los usuarios, haciéndolas irreversibles.

4.2.2. Flujo del proceso de inicio de sesión:

Estructura de carga útil:

DNI (dni): Cadena de identificación del usuario.
Contraseña (contraseña): Cadena de contraseña del usuario.
Autenticación de usuario:

El sistema verifica el DNI y la contraseña proporcionados con las credenciales almacenadas en la base de datos.
Si el DNI y la contraseña coinciden con una entrada de la base de datos, el usuario queda autenticado.

Código de verificación para médicos:

Para los usuarios médicos, un paso adicional podría implicar recibir un código de verificación.
Este código se puede enviar a través de correo electrónico.
El usuario debe ingresar el código recibido para completar el proceso de inicio de sesión.
Autorización de Acceso:

Tras una autenticación exitosa y una verificación del código (si corresponde), el sistema otorga acceso según la función y los permisos del usuario.
Inicialización de sesión:

El sistema crea una sesión o token para el usuario autenticado, lo que le permite acceder a las funciones del sistema sin volver a autenticarse durante un período específico.
Manejo de respuestas:

Genere y devuelva una respuesta adecuada que indique el éxito o el fracaso del intento de inicio de sesión.
Proporcione un token de acceso o un identificador de sesión al iniciar sesión correctamente para interacciones posteriores con el sistema.

4.2.3. Flujo de datos de actualización de información del usuario:

Datos de entrada:

DNI (dni): Número de identificación vigente del usuario.
Nuevo DNI (new_dni): Número de identificación actualizado del usuario (si procede).
Nombre (nombre): Nombre actualizado del usuario.
Rol ID (rol_id): Identificador de rol actualizado para el usuario.
ID de establecimiento (establecimiento_id): Identificador de establecimiento actualizado para el usuario.

Especialidad (especialidad): Especialización actualizada para el usuario.

Validación:

Garantizar la exactitud y el formato de los datos proporcionados.
Desinfecte las entradas de datos para evitar vulnerabilidades de seguridad.
Proceso de actualización:

Ejecuta una consulta de actualización o llamada API para modificar la información del usuario en la base de datos del sistema.
Actualizar la información del usuario en función de los parámetros proporcionados (nuevo DNI, nombre, rol, establecimiento, especialización).

Manejo de respuestas:

Generar una respuesta indicando el éxito o fracaso del proceso de actualización.
Devuelva un mensaje apropiado indicando el estado de la actualización al administrador.

4.2.4. Flujo de datos para restablecer contraseña:

Entrada del usuario:

DNI (dni): Número de identificación del usuario con el que se inicia el restablecimiento de la contraseña.
Generación de código de correo electrónico:

Al recibir el DNI, el sistema genera un código único.
Este código se envía al correo electrónico del usuario para su verificación.
Verificación de código:

El usuario envía el código recibido para su validación.
El sistema compara el código ingresado con el código almacenado para su validación.
Creación de JWT:

Tras la verificación exitosa del código:
El sistema genera un token web JSON (JWT) que contiene un identificador único o información específica del usuario.
Este JWT sirve como credencial temporal para el proceso de restablecimiento de contraseña.
Almacenamiento de tokens:

El JWT generado se almacena de forma segura en la base de datos, asociado con la cuenta del usuario o el identificador único.
Solicitud de restablecimiento de contraseña:

El usuario envía una nueva contraseña junto con el JWT recibido para restablecer la contraseña.
Comparación de tokens:

El sistema compara el JWT enviado por el usuario con el JWT almacenado en la base de datos.
Actualización de contraseña:

Si los tokens coinciden:
El sistema actualiza la contraseña del usuario en la base de datos con la nueva contraseña proporcionada por el usuario.
Manejo de respuestas:

Se genera una respuesta que indica el éxito o el fracaso del proceso de restablecimiento de contraseña.
Se envía un mensaje apropiado al usuario confirmando la actualización de la contraseña o solicitando un nuevo intento en caso de falla.

4.2.5. Flujo de datos de eliminación de usuarios:

Datos de entrada:

DNI (dni): Número de identificación del usuario para especificar el usuario a eliminar.
Solicitud de eliminación:

El usuario envía una solicitud para eliminar su cuenta o un administrador inicia una solicitud de eliminación basada en el DNI del usuario.
Validación del DNI:

El sistema valida el formato y existencia del DNI aportado.
Garantiza que el DNI proporcionado para su eliminación coincide con una cuenta de usuario existente.
Proceso de eliminación:

Tras la validación exitosa:
El sistema ejecuta una consulta de eliminación o llamada API dirigida al usuario asociado al DNI proporcionado.
La cuenta de usuario vinculada al DNI aportado se elimina definitivamente de la base de datos del sistema.
Manejo de respuestas:

Generar una respuesta indicando el éxito o fracaso del proceso de eliminación.
Proporcione un mensaje apropiado confirmando la eliminación o notificando si la eliminación no tuvo éxito.

4.2.6. Recuperación de Información del Usuario mediante Flujo de Datos DNI:

Datos de entrada:

DNI (dni): Número de identificación del usuario utilizado como parámetro para recuperar la información del usuario.
Solicitud de recuperación de información:

El usuario o sistema inicia una solicitud para recuperar información del usuario en función del DNI proporcionado.
Validación del DNI:

El sistema valida el formato y existencia del DNI aportado.
Garantiza que el DNI proporcionado corresponde a una cuenta de usuario existente.
Ejecución de consultas:

Tras la validación exitosa:
El sistema ejecuta una consulta o llamada API para obtener información del usuario asociada al DNI proporcionado.
Recupera detalles como nombre, correo electrónico, función, establecimiento o cualquier otra información pertinente vinculada a la cuenta de usuario.
Compilación de información:

La información del usuario recuperada se compila en un formato de respuesta adecuado.
Generación de respuesta:

Genere una respuesta que contenga la información del usuario recuperada.
Proporcione un mensaje apropiado que contenga detalles del usuario o notifique si la recuperación de la información del usuario no tuvo éxito.

4.2.7. Flujo de datos de contacto:

Datos de entrada:

Nombre y Apellido (nombre_apellido): Nombre y apellidos de la persona que recibe el mensaje.
Correo electrónico (email): Dirección de correo electrónico del destinatario.
Mensaje (mensaje): El mensaje a enviar.
Envío de mensajes:

Un médico envía un mensaje de contacto destinado a una persona específica, proporcionando su nombre, correo electrónico y el mensaje en sí.
Validación de datos:

El sistema valida el formato y la corrección del correo electrónico proporcionado.
Garantiza que el correo electrónico proporcionado esté en un formato válido para la comunicación.
Almacenamiento de mensajes:

Tras la validación exitosa:
El sistema almacena el mensaje enviado junto con el nombre del destinatario, el correo electrónico y el contenido del mensaje en una tabla de base de datos diseñada específicamente para almacenar mensajes de contacto.
Respuesta de confirmación:

Generar una respuesta indicando el éxito o fracaso del guardado del mensaje.

4.3. Feedback flujo de datos

El feedback es hecho por un médico al recibir un diagnóstico de un modelo y da un feedback sobre lo que quiere hacer.

4.3.1. Flujo de datos de envío dar un feedback del diagnóstico del cerebro :

Datos de entrada:

Imagen ID (imagen_id): Identificador que se vincula a la imagen concreta utilizada para el diagnóstico.
glioma: Booleano que indica la presencia de glioma en el diagnóstico.
meningioma: Booleano que indica la presencia de meningioma en el diagnóstico.
pituitaria: booleano que indica la presencia de problemas hipofisarios en el diagnóstico.
no_tumor: booleano que indica que no hay presencia de tumor en el diagnóstico.
Comentario del médico (comentario): Comentario del médico sobre el diagnóstico.

Envío de comentarios:

Un médico envía comentarios relacionados con el diagnóstico realizado por el modelo.
El médico especifica los detalles relevantes como la identificación de la imagen, la presencia de diferentes condiciones y agrega un comentario.

Validación de datos:

El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.
Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.

Almacenamiento de comentarios:

Tras la validación exitosa:

El sistema almacena los comentarios enviados en una tabla o estructura de base de datos dedicada diseñada para registrar comentarios relacionados con los diagnósticos.
Registra la identificación de la imagen, las afecciones diagnosticadas (p. ej., glioma, meningioma, hipófisis, ningún tumor) y el comentario del médico.
Generación de respuesta:

Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de los comentarios o notifique si el envío no tuvo éxito.

4.3.2. Flujo de datos de envío de comentarios sobre el corazón:

Datos de entrada:

Imagen ID (imagen_id): Identificador que vincula a la imagen específica utilizada para el diagnóstico del corazón.
Contracción ventricular prematura: booleano que indica contracciones ventriculares prematuras.
Fusión de latido ventricular y normal: booleano que indica fusión de latidos ventriculares y normales.
Infarto de miocardio: booleano que indica infarto de miocardio.
Latido no clasificable: booleano que indica latidos no clasificados.
Latido normal: booleano que indica un latido cardíaco normal.
Latido prematuro supraventricular: booleano que indica latido prematuro supraventricular.
Este es un comentario de corazón: Comentario del médico sobre el diagnóstico del corazón.
Envío de comentarios:

Un médico envía comentarios relacionados con el diagnóstico cardíaco realizado, especificando detalles como identificación de imagen, diversas afecciones cardíacas y agregando comentarios.
Validación de datos:

El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.

Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.
Almacenamiento de comentarios:

Tras la validación exitosa:
El sistema almacena los comentarios relacionados con el corazón enviados en una tabla o estructura de base de datos dedicada diseñada para registrar dichos comentarios.
Registra la identificación de la imagen, las afecciones cardíacas diagnosticadas y el comentario del médico.
Generación de respuesta:

Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de los comentarios relacionados con el corazón o notifique si el envío no tuvo éxito.

4.3.3. Flujo de datos de envío de comentarios de muñeca:

Datos de entrada:

Imagen ID (imagen_id): Identificador que vincula a la imagen concreta utilizada para el diagnóstico de la muñeca.
Fractura: Booleano que indica la presencia de una fractura.
Sano: Booleano que indica una condición saludable (sin fractura).
Comentario del médico (comentario): Comentario del médico sobre el diagnóstico de la muñeca.
Envío de comentarios:

Un médico envía comentarios relacionados con el diagnóstico de muñeca realizado, especificando detalles como identificación por imagen, presencia de una fractura, estado de salud y agregando comentarios.

Validación de datos:

El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.
Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.

Almacenamiento de comentarios:

Tras la validación exitosa:
El sistema almacena los comentarios enviados relacionados con la muñeca en una tabla o estructura de base de datos dedicada diseñada para registrar dichos comentarios.
Registra la identificación de la imagen, las condiciones diagnosticadas (fracturadas o sanas) y el comentario del médico.

Generación de respuesta:

Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de los comentarios relacionados con la muñeca o notifique si el envío no tuvo éxito.

4.3.4. Flujo de datos de envío de comentarios de pulmón:

Datos de entrada:

Imagen ID (imagen_id): Identificador que vincula a la imagen específica utilizada para el diagnóstico pulmonar.
Neumonía: Booleano que indica la presencia de neumonía.
Sin neumonía: booleano que indica ausencia de neumonía.
Comentario: Comentario del médico sobre el diagnóstico de pulmón.

Envío de comentarios:
Un médico envía comentarios relacionados con el diagnóstico pulmonar realizado, especificando detalles como identificación por imagen, presencia de neumonía, ausencia de neumonía y agregando comentarios.

Validación de datos:
El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.
Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.

Almacenamiento de comentarios:
Tras la validación exitosa:
El sistema almacena los comentarios relacionados con los pulmones enviados en una tabla o estructura de base de datos dedicada diseñada para registrar dichos comentarios.
Registra la imagen de identificación, las condiciones diagnosticadas (neumonía o ausencia de neumonía) y el comentario del médico.

Generación de respuesta:
Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de la retroalimentación relacionada con los pulmones o notifique si el envío no tuvo éxito.

4.3.5. Flujo de datos de envío de comentarios sobre los riñones:

Datos de entrada:

Imagen ID (imagen_id): Identificador que vincula a la imagen específica utilizada para el diagnóstico renal.
Quiste: Booleano que indica la presencia de un quiste en el riñón.
Piedra: Booleano que indica la presencia de un cálculo renal.
Tumor: Booleano que indica la presencia de un tumor en el riñón.
Normal: Booleano que indica una condición normal sin anomalías en el riñón.
Comentario: Comentario del médico sobre el diagnóstico del riñón.

Envío de comentarios:

Un médico envía comentarios relacionados con el diagnóstico renal realizado, especificando detalles como identificación por imagen, presencia de un quiste, cálculo renal, tumor, condición normal y agregando comentarios.

Validación de datos:

El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.
Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.

Almacenamiento de comentarios:

Tras la validación exitosa:
El sistema almacena los comentarios enviados relacionados con los riñones en una tabla o estructura de base de datos dedicada diseñada para registrar dichos comentarios.
Registra la identificación de la imagen, las condiciones diagnosticadas (quiste, cálculo renal, tumor, condición normal) y el comentario del médico.

Generación de respuesta:

Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de los comentarios relacionados con los riñones o notifique si el envío no tuvo éxito.

4.3.6. Flujo de datos de envío de comentarios sobre rodillas:

Datos de entrada:

Imagen ID (imagen_id): Identificador que vincula a la imagen específica utilizada para el diagnóstico de rodilla.
Rotura LCA: booleano que indica la presencia de un ligamento cruzado anterior (LCA) desgarrado.
LCA Sano: Booleano que indica un ligamento cruzado anterior (LCA) sano o intacto.
Comentario del médico (comentario): Comentario del médico sobre el diagnóstico de rodilla.
Envío de comentarios:

Un médico envía comentarios relacionados con el diagnóstico de rodilla realizado, especificando detalles como la identificación de la imagen, la presencia de un ligamento cruzado anterior desgarrado, un ligamento cruzado anterior sano y agregando comentarios.

Validación de datos:

El sistema valida la entrada, asegurando la exactitud de la identificación de la imagen y los valores booleanos proporcionados.
Verifica que la ID de la imagen proporcionada corresponda a una imagen existente en la base de datos.
Almacenamiento de comentarios:

Tras la validación exitosa:
El sistema almacena los comentarios enviados relacionados con la rodilla en una tabla o estructura de base de datos dedicada diseñada para registrar dichos comentarios.
Registra la identificación de la imagen, las condiciones diagnosticadas (LCA desgarrado, LCA sano) y el comentario del médico.

Generación de respuesta:

Genere una respuesta que confirme el éxito o el fracaso del envío de comentarios.
Proporcione un mensaje apropiado que confirme la adición exitosa de los comentarios relacionados con la rodilla o notifique si el envío no tuvo éxito.

5. Cifrado de datos y medidas de seguridad en la base de datos

Esta sección de la documentación de la base de datos proporciona una descripción detallada de las estrategias de cifrado implementadas para proteger datos confidenciales, que incluyen direcciones de correo electrónico cifradas, imágenes almacenadas como bytea y contraseñas hash dentro de nuestro sistema de base de datos. La documentación tiene como objetivo garantizar el cumplimiento de los estándares de seguridad, salvaguardar la información confidencial y mitigar los riesgos potenciales asociados con el acceso no autorizado o las violaciones de datos.

5.1. Email

- Campo: email

- Método de cifrado: algoritmo de cifrado AES-256
- Proceso de cifrado: los correos electrónicos se cifran utilizando una clave de cifrado única generada para cada correo electrónico antes de almacenarse en la columna "email" de la tabla "usuarios". El descifrado se produce tras la autenticación del usuario.
- Administración de claves: las claves de cifrado se almacenan de forma segura en un sistema de administración de claves independiente, al que solo pueden acceder los administradores autorizados. Las claves se rotan periódicamente siguiendo las políticas de seguridad de la empresa.
- Uso y acceso: solo los administradores del sistema autorizados tienen acceso a las claves de cifrado para fines de mantenimiento o recuperación. Los usuarios habituales no pueden acceder ni ver los datos del correo electrónico descifrados.
- Controles de acceso a datos: el acceso al campo 'email' está restringido mediante el control de acceso basado en roles (RBAC), lo que garantiza que solo roles específicos tengan permiso para ver o modificar datos de correo electrónico cifrados.
- Medidas de seguridad: los correos electrónicos cifrados se transmiten a través de canales seguros y se almacenan en un formato cifrado para mitigar posibles amenazas a la seguridad.
- Cumplimiento y regulaciones: las prácticas de cifrado cumplen con los estándares de la industria y las regulaciones de privacidad de datos relevantes.
- Recuperación ante desastres: existen planes de contingencia para recuperar claves de cifrado o datos cifrados en caso de emergencias o eventos de pérdida de datos, garantizando la continuidad del negocio.

5.2. Imágenes

- Este campo almacena imágenes en formato binario dentro de la base de datos.
- Proceso de almacenamiento de imágenes:
    - Las imágenes cargadas en la base de datos se almacenan directamente como datos binarios (bytea).
    - Al cargarlas, las imágenes se almacenan como datos binarios sin formato y sin cifrado.
- Controles de acceso:

    - Acceso autorizado:
        - El acceso al campo imagen está controlado por los permisos de la base de datos, lo que limita la modificación o recuperación a usuarios o procesos autorizados.
- Medidas de seguridad:
    - Transmisión y Almacenamiento:
        - Las imágenes binarias se transmiten y almacenan de forma segura mediante conexiones o protocolos cifrados para garantizar una transferencia de datos segura.
        - El servidor de la base de datos emplea protocolos de seguridad estándar y controles de acceso para salvaguardar las imágenes binarias almacenadas.

5.3. Password

- Campo: password
- Propósito: Este campo almacena contraseñas de usuario con hash en formato hexadecimal dentro de la base de datos.
- Proceso de hash de contraseña:
    - Algoritmo de hash y codificación:
    - Las contraseñas se codifican mediante un algoritmo de hash sólido (SHA-256).
    - El hash resultante se codifica en formato hexadecimal antes del almacenamiento.
- Características clave:
    - Método de codificación:
        - Las contraseñas hash se representan como cadenas de caracteres hexadecimales, lo que garantiza la compatibilidad y la facilidad de almacenamiento dentro de la base de datos.
- Controles de acceso:
    - Acceso restringido:
        - El acceso limitado a contraseñas hash se otorga únicamente a componentes autorizados del sistema o personal con permisos específicos.
- Medidas de seguridad:
    - Confidencialidad e Integridad:
        - El almacenamiento de contraseñas en formato hexadecimal garantiza la integridad y confidencialidad de los datos.

        - La codificación hexadecimal ayuda a mantener la seguridad de las contraseñas hash al proporcionar una representación coherente y legible por máquina.
    - Cumplimiento:
        - Cumplimiento normativo:
            - El almacenamiento de contraseñas hash en formato hexadecimal se alinea con las prácticas de seguridad estándar de la industria y los requisitos reglamentarios relacionados con la protección de contraseñas y el almacenamiento de datos confidenciales.

6. Niveles de acceso y roles:

- Superusers:
    - Benítez, Micaela.
    - Benítez, Yamila.
    - Cláuser, Nahuel.
    - Gómez, Federico.
    - Pérez, Gianina.
    - Prieto, Lucas.
    - Torrico, Franco
- Descripción del rol:
    - Superusers: las personas enumeradas anteriormente tienen los mismos niveles de acceso y roles dentro del sistema. Poseen amplios privilegios para realizar tareas administrativas, acceder

a datos confidenciales y gestionar diversas funcionalidades dentro de la base de datos.

- Nivel de acceso:
  - Acceso total: los superusers tienen acceso ilimitado a todas las áreas de la base de datos, incluidos privilegios de lectura, escritura, ejecución y administrativos. Pueden realizar tareas como manipulación de datos, cambios de configuración y mantenimiento del sistema sin limitaciones.
- Responsabilidades:
  - Administración del sistema: los superusuarios son responsables de supervisar el funcionamiento de la base de datos, gestionar el acceso de los usuarios, implementar medidas de seguridad y garantizar el buen funcionamiento del sistema.
- Control de acceso:
  - Autorización: A todas las personas enumeradas se les ha otorgado acceso de superusuario para satisfacer las necesidades operativas y los requisitos administrativos del sistema.
- Nota:
  - Acceso uniforme: cada individuo enumerado tiene un nivel equivalente de acceso y responsabilidad dentro del sistema como superusers.

7. Tareas de mantenimiento de rutina

7.1. Backup

- Frecuencia: Copias de seguridad semanales durante las horas de menor actividad para minimizar el impacto en las operaciones en vivo.
- Tipos: Copias de seguridad completas semanales para reducir la duración de las copias de seguridad y los requisitos de almacenamiento.
- Almacenamiento: almacenamiento externo en una plataforma segura en la nube con copias redundantes para recuperación ante desastres.(Hosteada en render)
- Procedimientos: Copias de seguridad mediante trabajos programados utilizando utilidades PostgreSQL con verificaciones manuales periódicas.

- Seguridad: Cifrado de archivos de respaldo mediante cifrado AES-256 y estrictos controles de acceso que limitan el acceso al personal autorizado.
- Revisión: auditorías trimestrales para revisar los registros de respaldo, probar los procedimientos de restauración y actualizar la documentación de la estrategia de respaldo.

7.2. Procedimientos de actualización

- Comprobaciones previas a la actualización:
    - Backup:
    - Copia de seguridad completa: realice una copia de seguridad completa de la base de datos existente antes de iniciar la actualización.
    - Verificación: confirme la integridad de la copia de seguridad restaurándola en un entorno de prueba.
    - Revisar las notas de la versión:
        - Comprensión de los cambios: revise detenidamente las notas de la versión de la nueva versión de la base de datos para comprender los cambios, las mejoras y las posibles incompatibilidades.
    - Requisitos del sistema:
        - Verificar compatibilidad: asegúrese de que la nueva versión sea compatible con el entorno de hardware y software existente.
        - Verificación de recursos: evalúe si el sistema cumple con los nuevos requisitos de recursos introducidos en la versión actualizada.

    - Pruebas de compatibilidad:
        - Entorno de prueba: configure un entorno de prueba para simular el proceso de actualización y evaluar la compatibilidad con las aplicaciones existentes.
        - Pruebas de funcionalidad: verifique que las funciones y aplicaciones críticas funcionen sin problemas en la nueva versión.

- Requisitos previos:
    - Dependencias de software:

        - Actualizar dependencias: asegúrese de que todos los componentes de software que interactúan con la base de datos sean compatibles con la nueva versión.

        - Actualizar controladores: actualiza los controladores de la base de datos si es necesario para la conectividad de la aplicación.
- Plan de Migración de Datos:
    - Evaluación de datos: evaluar las estructuras y formatos de datos para identificar cualquier cambio que pueda afectar la migración de datos.

- Proceso de actualización:
    - Detener los servicios de base de datos:
        - Terminación del servicio: detenga los servicios de base de datos existentes para evitar modificaciones de datos durante la actualización.
    - Instalación del software de base de datos:

    - Instalación de nuevo software: instale la nueva versión del software de la base de datos en el servidor.
- Configuración:

    - Conservar configuración: conserva los ajustes de configuración críticos de la versión anterior.
    - Actualizar configuraciones: modifique las configuraciones si es necesario según los requisitos de la nueva versión.
- Migración de datos:
    - Ejecución de la migración: ejecutar el plan de migración de datos desarrollado durante la fase de requisitos previos.
    - Validación: verificar la integridad y precisión de los datos migrados.
- Actualizaciones de esquema:
    - Ajustes manuales: realice los ajustes manuales necesarios para adaptarse a los cambios de esquema.
- Iniciar servicios de base de datos:
    - Reanudación del servicio: reinicie los servicios de la base de datos para que la versión actualizada esté operativa.
- Verificación posterior a la actualización:
    - Pruebas funcionales:
        - Funciones críticas: pruebe funciones y aplicaciones críticas para asegurarse de que funcionen como se espera.
        - Pruebas de aceptación del usuario: involucrar a los usuarios finales en el proceso de prueba para validar la experiencia del usuario.
- Pruebas de rendimiento:
    - Rendimiento de las consultas: evalúe el rendimiento de las consultas para garantizar que cumpla con las expectativas.

        - Utilización de recursos: supervise la utilización de recursos (CPU, memoria, disco) para identificar posibles cuellos de botella.
    - Confirmación de copia de seguridad:
        - Copia de seguridad posterior a la actualización: realice una copia de seguridad de la base de datos actualizada para establecer un punto de recuperación posterior a la actualización.
    - Configuración de monitoreo:
        - Alertas y monitoreo: configure alertas y herramientas de monitoreo para detectar cualquier problema o anomalía en el entorno posterior a la actualización.

8. Escenarios de falla

- Fallo de hardware:
    - Descripción del escenario:
        - Tipo: los componentes de hardware críticos (por ejemplo, unidades de almacenamiento, componentes del servidor) fallan inesperadamente.
        - Impacto: Baja inmediata de servicios de bases de datos críticos.
        - Mitigación: implementar mecanismos de redundancia o conmutación por error para reducir el impacto de las fallas de hardware.
        - Priorización de riesgos:
        - Gravedad: Alta
        - Probabilidad: moderada a alta (según la antigüedad del hardware y el historial de mantenimiento)
        - Prioridad de mitigación: Urgente

- Ataques cibernéticos:
    - Descripción del escenario:
        - Tipo: malware, ransomware, ataques DDoS o violaciones de datos dirigidas a la base de datos.
        - Impacto: robo de datos, corrupción de datos o interrupción del servicio.
        - Mitigación: Medidas sólidas de ciberseguridad, cifrado y sistemas de detección de intrusiones.
        - Priorización de riesgos:
        - Gravedad: alta a muy alta
        - Probabilidad: moderada a alta (con amenazas cibernéticas en evolución)
        - Prioridad de mitigación: inmediata

- Error humano:
    - Descripción del escenario:
        - Tipo: Eliminación accidental de datos críticos, configuración incorrecta o actualizaciones inadecuadas.
        - Impacto: Pérdida de datos, interrupción del servicio o integridad de los datos comprometida.
        - Mitigación: controles de acceso estrictos, copias de seguridad periódicas y programas de capacitación para empleados.
        - Priorización de riesgos:
        - Gravedad: moderada a alta
        - Probabilidad: Moderada (debido a la participación humana)
        - Prioridad de mitigación: capacitación continua y mejora de procesos

- Fallos o errores de software:
    - Descripción del escenario:
        - Tipo: fallos, errores o problemas de compatibilidad del software de base de datos.
        - Impacto: interrupción del servicio, inconsistencia de los datos o resultados de consulta incorrectos.
        - Mitigación: actualizaciones periódicas de software, pruebas y protocolos de corrección de errores.
        - Priorización de riesgos:
        - Gravedad: moderada a alta
        - Probabilidad: Moderada (especialmente con sistemas de software complejos)
        - Prioridad de mitigación: actualizaciones programadas y monitoreo continuo

- Resumen de priorización de riesgos:

- Alta gravedad, alta probabilidad: se necesita atención inmediata y estrategias sólidas de mitigación.
- Gravedad alta, probabilidad moderada: monitoreo continuo y medidas proactivas para mitigar los riesgos.
- Gravedad moderada, alta probabilidad: controles periódicos, formación y mecanismos de prevención.
- Gravedad moderada a baja, probabilidad baja: concientización y seguimiento, con revisiones periódicas y actualizaciones de los protocolos.

9.