Tarea: Una vez que el usuario se autentica en función de sus roles, se decide a qué rutas se puede acceder. Por ejemplo: Una ruta para consultar qué convocatorias están abiertas tiene que estar visible para todos los usuarios con el rol de Estudiante, pero un usuario con este rol no podrá modificar las convocatorias, esta sería una tarea solamente de los administradores del sistema.

Actor: Estudiante
Rol del sistema: Estudiante
Rol base de datos: Estudiante
Descripción: Puede visualizar las vistas correspondientes a la información, solicitudes y perfil de usuario.
Descripción base de datos: Realiza la solicitud de intercambio
Permisos base de datos: Lectura y edición

Actor: Aprobador administrativo
Rol del sistema: Aprobador administrativo
Rol base de datos: Aprobador administrativo
Descripción: Puede visualizar las vistas correspondientes a la información y solicitudes de los estudiantes.
Descripción base de datos: Tiene acceso a las solicitudes de los estudiantes.
Permisos base de datos: Lectura y edición

Actor: Administrador
Rol del sistema: Administrador del sistema
Rol base de datos: Administrador del sistema
Descripción: Puede visualizar las vistas de administración del sistema y control de usuarios.
Descripción base de datos: Tiene acceso a todo.
Permisos base de datos: Escritura, lectura y edición

Actor: Consultor
Rol del sistema: Consultor del sistema
Rol base de datos: Consultor
Descripción: Puede visualizar las vistas de administración del sistema y control de usuarios.
Descripción base de datos: Puede únicamente ver todo
Permisos base de datos: Lectura

Un rol de aplicación consta de un juego de privilegios que determinan lo que los usuarios pueden ver y hacer después de conectarse a MySQL. El trabajo de administrador consiste en asignar usuarios a uno o varios roles de aplicación.

Existen dos tipos de roles de aplicación:

1. Predefinido: Privilegios fijos definidos inicialmente
2. Definido por el usuario: Creado por administradores. Incluye uno o varios roles de aplicación predefinidos.

Posibles nuevos roles para la gestión de base de datos:

Administrador de servicio de DB	Permite a los usuarios administrar la base de datos y delegar los privilegios a otros usuarios.	Administrador de dominio de identidad
Autor de modelo de datos de DB	Permite a los usuarios gestionar el modelo de datos en la base de datos.	Administrador de servicio de DB
Autor de carga de datos de DB	Permite a los usuarios cargar los datos y la sincronización a la base de datos.	Administrador de servicio de DB
Autor de contenido de DB	Permite a los usuarios crear análisis en la base de datos.	Autor de modelo de datos de DB
Consumidor de DB	Permite a los usuarios ver y ejecutar informes en la base de datos. Rol de aplicación para controlar quién tiene acceso al servicio.	Autor de contenido de DB

Método de gestión de permisos y roles: JWT (*JSON Web Token*)

Un JSON Web Token (*JWT*) es un estándar abierto que define una forma compacta y autónoma para transmitir de forma segura información entre las partes como un objeto JSON. Esta información puede ser verificada y confiable porque está firmada digitalmente. Una vez que el usuario haya iniciado sesión, cada solicitud incluirá el JWT, lo que permitirá al usuario acceder a las rutas, servicios y recursos que se permiten con ese token.