Diseño de Base de Datos - TaskManager

**Fecha:10/09/2025**

**Autor:** Raurau Quispe, Juan Boris; Munares Chamorro, Juan Carlos

**Versión:** 2.0

# 1. Introducción

Este documento describe el modelo de base de datos relacional para el sistema SISTEC, enfocado en la gestión de seguridad y monitoreo de equipos de laboratorio mediante tecnología RFID. Se detallan las entidades principales, relaciones, restricciones, diccionario de datos y consideraciones técnicas para la implementación en MySQL/MariaDB.

# 2. Diagrama Entidad-Relación (ERD)

## 2.1. Entidades y sus Atributos

1. usuarios

- id (PK)

- usuario (único)

- contrasena

- rol (admin, tecnico, invitado)

2. equipos

- id (PK)

- nombre

- ubicacion

- estado (Autorizado, No autorizado)

- fecha\_registro

- numero\_tarjeta\_rfid (único)

3. alertas

- id (PK)

- mensaje

- ubicacion

- nivel (peligro, cuidado)

- fecha

- numero\_tarjeta\_rfid (FK, referencia a equipos)

## 2.2. Relaciones

* Un equipo puede generar múltiples alertas, pero cada alerta está asociada a un único equipo a través de `numero\_tarjeta\_rfid`.
* La relación entre equipos y alertas es de uno a muchos (1:N).

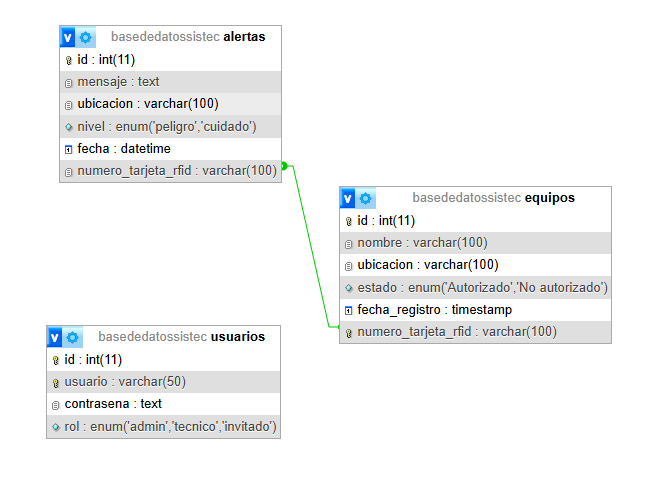
## 2.3. Reglas y Restricciones

* El campo `usuario` en la tabla `usuarios` debe ser único.
* El campo `numero\_tarjeta\_rfid` en la tabla `equipos` debe ser único.
* La FK `alertas.numero\_tarjeta\_rfid` referencia a `equipos.numero\_tarjeta\_rfid` con eliminación SET NULL.

## 2.4. Diagrama de Base de Datos (E/R)

* usuarios
* equipos (1) ─> (N) alertas (Relación: Un equipo puede generar muchas alertas)

# 3. Diagrama Relacional



# 4. Diccionario de Datos

**Tabla Usuarios**

| Campo | Tipo de Dato | Descripción | Restricciones |
| --- | --- | --- | --- |
| id | INT(11) | Identificador único del usuario. | PRIMARY KEY, AUTO\_INCREMENT |
| usuario | VARCHAR(50) | Nombre completo para login | UNIQUE, NOT NULL |
| contrasena | TEXT | Hash de contraseña. | NOT NULL |
| rol | ENUM('admin','tecnico','invitado') | Rol del usuario para control de acceso | NOT NULL, DEFAULT ‘invitado’ |

**Tabla Equipos**

| Campo | Tipo de Dato | Descripción | Restricciones |
| --- | --- | --- | --- |
| Id\_Equipos | INT1(11) | Identificador único del equipo | PRIMARY KEY, AUTO\_INCREMENT |
| Nombre\_equipo | VARCHAR(100) | Nombre descriptivo del equipo | NOT NULL |
| Ubicacion | VARCHAR(100) | Ubicación fisica del eiquipo | NOT NULL |
| estado | ENUM('autorizado','no autorizado') | Estado autorización del equipo | NOT NULL, DEFAULT ‘Autorizado’ |
| Fecha\_registro | TIMESATAMP | Fecha y hora de registro | NOT NULL, DEFAULT CURRENT\_TIMESTAMP |
| Numero\_tarjeta\_rfid | VARCHAR(100) | UID de la tarjeta RFID | UNIQUE, NOT NULL |

**Tabla Alertas**

| Campo | Tipo de Dato | Descripción | Restricciones |
| --- | --- | --- | --- |
| id\_alertas | INT(11) | Identificador único de la alerta. | PRIMARY KEY, AUTO\_INCREMENT |
| mensaje | TEXT | Descripción textual del evento. | NOT NULL |
| ubicacion | VARCHAR(100) | Ubicación asociada | NULL |
| fecha | DATETIME | Marca temporal del evento | DEFAULT CURRENT\_TIMESTAMP |
| Numero\_tarjeta\_rfid | VARCHAR(100) | UID de la tarjeta RFID asociada | FOREIGN KEY (equipos) |

## 4.1. Relaciones y Restricciones:

* **Equipos ↔ Alertas (Relación 1:N):** Un equipo puede generar múltiples alertas, pero cada alerta está asociada a un único equipo. La relación está representada por el campo numero\_tarjeta\_rfid en la tabla alertas, que es una clave foránea (FK) que referencia al campo numero\_tarjeta\_rfid en la tabla equipos. La restricción de integridad referencial está configurada con ON DELETE SET NULL ON UPDATE CASCADE, lo que significa que si se elimina un equipo, las alertas asociadas se mantienen pero su referencia al equipo se establece en NULL, y si se actualiza el UID de un equipo, la change se propaga a las alertas.

# 5. Consideraciones de Escalabilidad

* **Índices en campos de búsqueda frecuente:** Se recomienda implementar índices en los campos utilizados frecuentemente en consultas y filtros, como numero\_tarjeta\_rfid en las tablas equipos y alertas, fecha en la tabla alertas para la generación de reportes históricos, y usuario en la tabla usuarios para el proceso de autenticación.
* **Uso de claves foráneas con políticas definidas:** La clave foránea alertas.numero\_tarjeta\_rfid que referencia a equipos.numero\_tarjeta\_rfid utiliza la política ON DELETE SET NULL. Esto permite preservar el historial de alertas en la base de datos incluso si un equipo es dado de baja (eliminado), manteniendo la integridad referencial para los registros existentes pero permitiendo la eliminación de equipos sin eliminar en cascada sus alertas históricas, lo cual es crucial para la auditoría.
* **Estrategias para grandes volúmenes de datos:** Para entornos con una cantidad muy alta de lecturas RFID, se debe considerar el **particionado** de la tabla alertas por rango de fechas (ej.: mensual). Esto mejorará significativamente el performance de las consultas y operaciones de mantenimiento sobre los datos históricos. Asimismo, se sugiere implementar un proceso de archivado automático que mueva las alertas antiguas (ej.: mayores a 1 año) a una tabla de almacenamiento frío (alertas\_historial).

# 6. Conclusiones

Este modelo relacional está diseñado para soportar los requisitos centrales del sistema SISTEC: el registro único de equipos, la trazabilidad completa de sus movimientos mediante alertas y la gestión segura de usuarios. La estructura propuesta es robusta, garantiza la integridad de los datos y permite escalar el sistema para manejar un crecimiento significativo en el número de equipos monitoreados y alertas generadas, todo ello sin comprometer el rendimiento ni la capacidad de auditoría.

.