

Cómo Casement mantiene separados los datos de cada empresa.

El problema de las bases de datos compartidas

Casement utiliza una base de datos compartida y multiinquilino: las propiedades, contratos e inquilinos de cada empresa viven en las mismas tablas. Es eficiente de operar, pero significa que un solo error en el código de la aplicación -- un filtro olvidado, una consulta copiada y pegada -- podría, en teoría, exponer los datos de una empresa a otra. Casement está construido para que ese error no pueda ocurrir, incluso si se comete.

Qué se aplica realmente

- **Seguridad a nivel de fila**

Postgres impone el aislamiento de inquilinos a nivel del motor de base de datos, en cada tabla de inquilino -- no como lógica de aplicación que un futuro error podría eludir.

- **Doble seguridad**

Cada consulta de inquilino también filtra explícitamente por ID de empresa en el código de la aplicación, además de la política a nivel de base de datos -- dos capas independientes, no una.

- **Un rol de ejecución restringido**

La aplicación se conecta a Postgres con un rol deliberadamente de bajos privilegios (`pms_app`), independiente del rol elevado usado solo para migraciones.

- **Autenticación por empresa**

Cada solicitud se autentica con un JWT que contiene la empresa del usuario, verificado en cada ruta protegida.