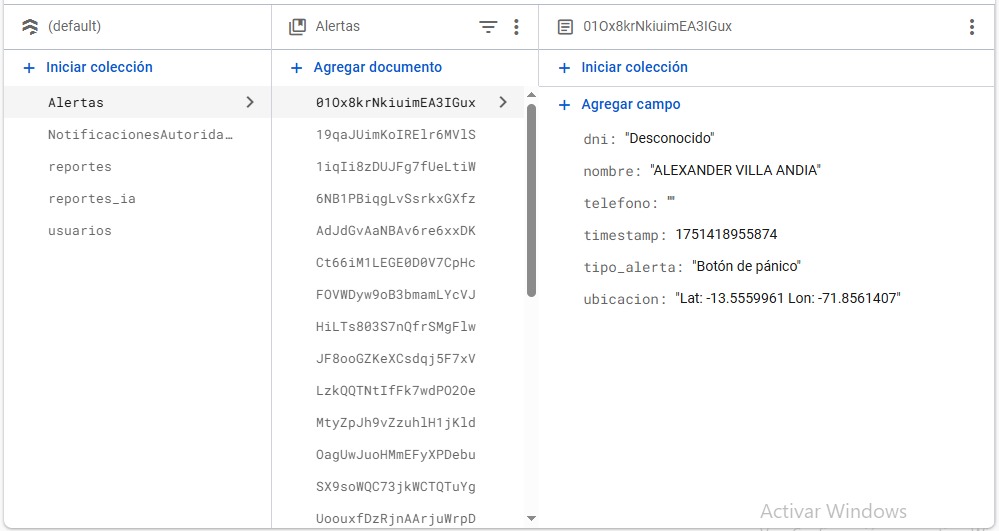
**COLECCIONES EN FIREBASE**

1. **Colección Alertas**

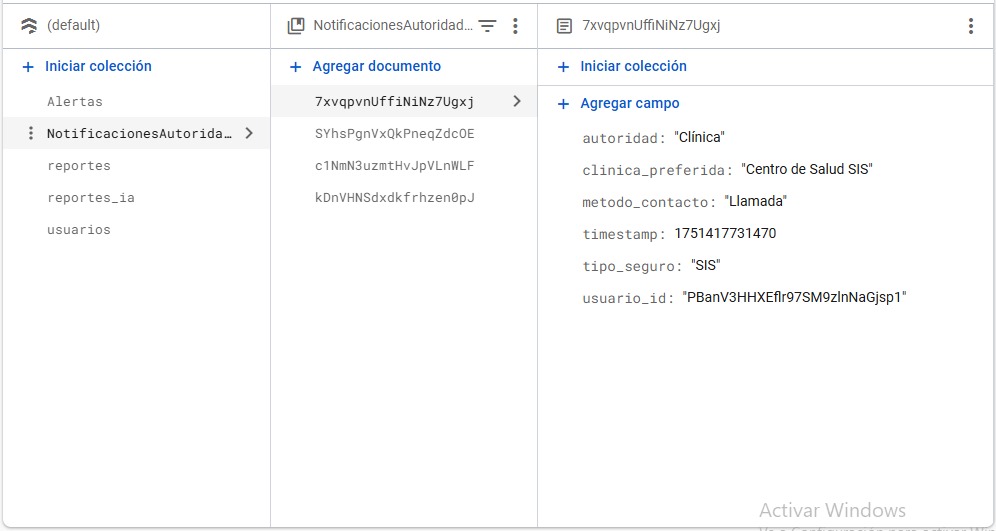


En esta colección se almacenó las alertas generadas por los usuarios.  
Cada documento dentro de Alertas contiene información básica del evento:

* **dni**: El documento de identidad del usuario (en este caso aparece como “Desconocido”).
* **nombre**: Nombre de la persona asociada a la alerta.
* **telefono**: Campo que puede contener el número del usuario.
* **timestamp**: Momento en el que se generó la alerta (en formato UNIX).
* **tipo\_alerta**: Describe el tipo de emergencia, aquí es un “Botón de pánico”.
* **ubicacion**: Coordenadas de latitud y longitud donde ocurrió la alerta.

Esta colección será la base para registrar y rastrear emergencias en tiempo real.

1. **Colección NotificacionesAutoridades**



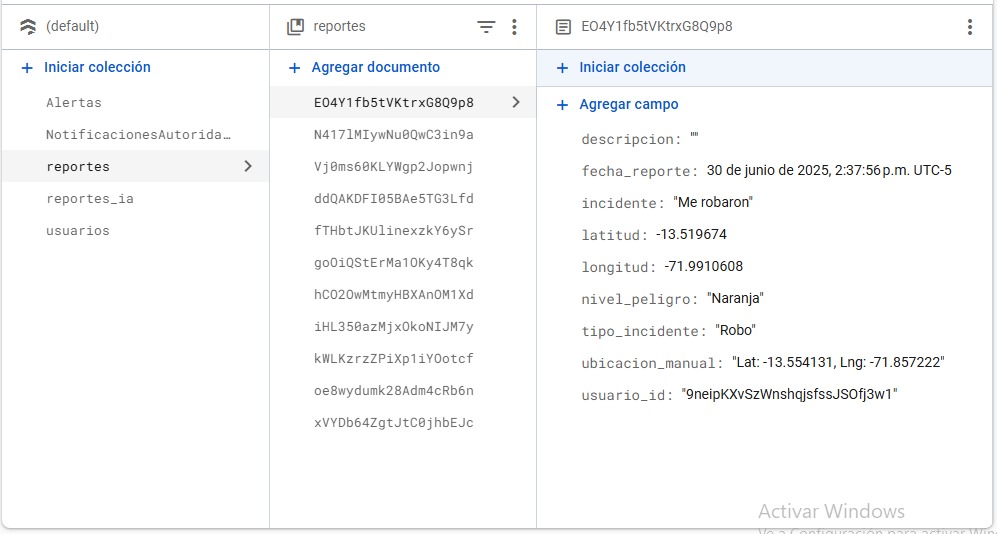
Aquí se configuró la información que será enviada a las autoridades o instituciones responsables cuando ocurre una alerta.

Los campos que definí son:

* **autoridad**: Tipo de entidad (por ejemplo, Clínica, Policía, Bomberos).
* **clinica\_preferida**: El centro de salud asignado o preferido.
* **metodo\_contacto**: Forma de contacto, en este caso “Llamada”.
* **timestamp**: Momento en que se registró la notificación.
* **tipo\_seguro**: Cobertura del usuario, aquí “SIS”.
* **usuario\_id**: Referencia al documento del usuario dentro de la colección usuarios.

Con esto se asegura que cada alerta tenga un canal de notificación definido para dar respuesta rápida.

1. **Colección reportes**



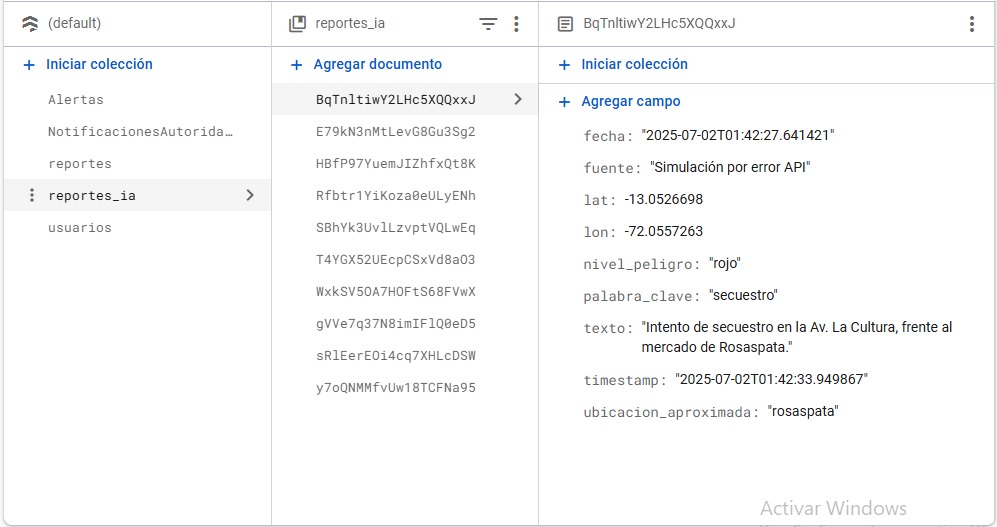
Aquí se organizó los reportes formales realizados por los usuarios sobre incidentes.

Cada documento contiene:

* **descripcion**: Detalles adicionales del reporte.
* **fecha\_reporte**: Fecha y hora en que el usuario realizó el reporte.
* **incidente**: Texto breve con lo sucedido (“Me robaron”).
* **latitud** y **longitud**: Coordenadas exactas del incidente.
* **nivel\_peligro**: Grado de severidad (por colores: verde, naranja, rojo).
* **tipo\_incidente**: Clasificación del evento (ejemplo: Robo).
* **ubicacion\_manual**: Ubicación registrada de forma manual.
* **usuario\_id**: Identificador que conecta con la colección de usuarios.

Esto permite llevar un historial de incidentes y clasificarlos por nivel de riesgo.

1. **Colección reportes\_ia**



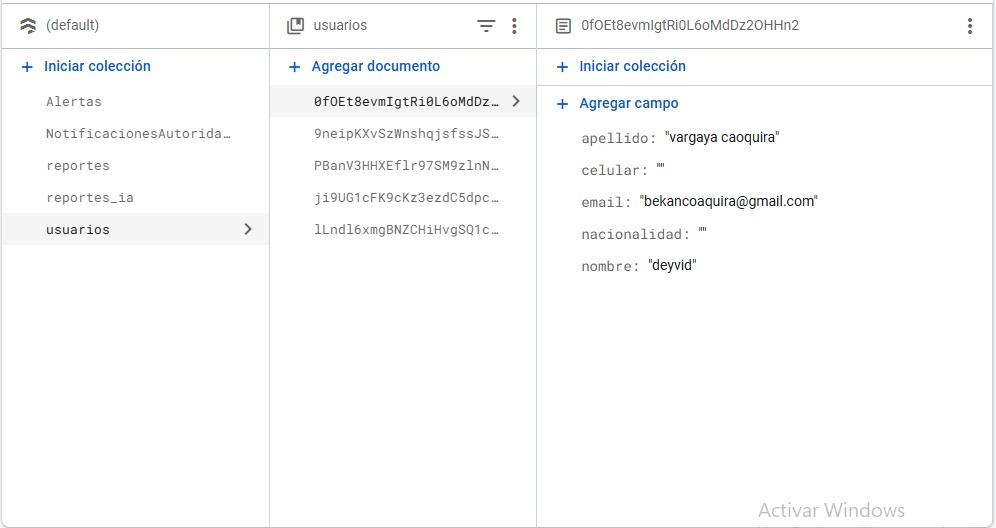
En esta parte se diseñó los reportes generados automáticamente por la inteligencia artificial (IA).

Los campos son:

* **fecha**: Fecha y hora de generación del reporte.
* **fuente**: De dónde proviene (por ejemplo, “Simulación por error API”).
* **lat** y **lon**: Ubicación estimada.
* **nivel\_peligro**: Nivel de alerta (ejemplo: rojo).
* **palabra\_clave**: Identificador clave detectado por la IA (ejemplo: “secuestro”).
* **texto**: Mensaje generado a partir del análisis de la IA.
* **timestamp**: Marca de tiempo.
* **ubicacion\_aproximada**: Dirección o zona referencial.

Esta colección complementa la anterior, ya que permite que la IA detecte posibles amenazas en tiempo real.

1. **Colección usuarios**



Finalmente, se configuró la base de datos de usuarios.

Cada documento incluye:

* **apellido**: Apellido del usuario.
* **celular**: Número telefónico.
* **email**: Correo electrónico de contacto.
* **nacionalidad**: País de origen.
* **nombre**: Nombre del usuario.

Esta colección es clave, porque centraliza la información de las personas que interactúan con el sistema y permite enlazarlas con alertas y reportes.