

Arquitectura

The Fraud Explorer está diseñado para permitir a sistemas de terceros consumir sus datos y realizar operaciones CRUD (**Create, Read, Update y Delete**) sobre sus registros tanto en la base de datos relacional como en la no estructurada.

A continuación en la tabla se resumen las capacidades de la arquitectura **REST** implementada en la solución:

Modulo	Operaciones disponibles
Endpoints	Leer datos de un Endpoint, leer todos los datos, crear un endpoint, eliminar un endpoint y actualizar el estado de un endpoint, teniendo en cuenta los permisos a través de la autenticación y su contexto.
Eventos y Alertas	Leer los eventos de un endpoint o de todos los endpoints presentados por el motor de Fraud Triangle Analytics. También se pueden leer las alertas generadas por el motor de inferencia del sistema de inteligencia artificial.
Workflows	Obtener el listado de los workflows existentes y obtener las alertas que han sido detectadas por los workflows. Los workflows son reglas que permiten crear una alerta si cumple con ciertas condiciones. Los workflows pueden correlacionar varias alertas y varias personas y es la forma más compleja y flexible de generación de alertas en The Fraud Explorer.
Triángulo del Fraude	Enviar datos de tipo semánticos para ser procesados en tiempo real y devolver los insights sobre el triángulo del fraude, incluyendo análisis de tono, relevancia, urgencia y probabilidad arrojada por la inteligencia artificial.
Model Context Protocol	Obtener un resumen general y detallado sobre las alertas de fraude y corrupción que ya han sido validadas no solo por FraudGPT sino por humanos. Estas alertas estarían listas para ser integradas en ciclos formales de User Behavior Analytics que lleve la empresa sobre todos los activos de la organización.

Se recomienda el uso del software **Postman**, en el cual deberá preparar el ambiente (Collections) para poder ejecutar las operaciones. Actualmente los métodos soportados son **GET, PUT, POST y DELETE**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones. Este software está siendo desarrollado por [NOFRAUD.la](#). Este contenido es privado y únicamente está disponible para clientes de NOFRAUD. Está prohibida su publicación en fuentes abiertas o disponibles al público.

Revision #5

Created 23 July 2025 03:15:04 by Julian Rios

Updated 25 July 2025 18:53:24 by Julian Rios