

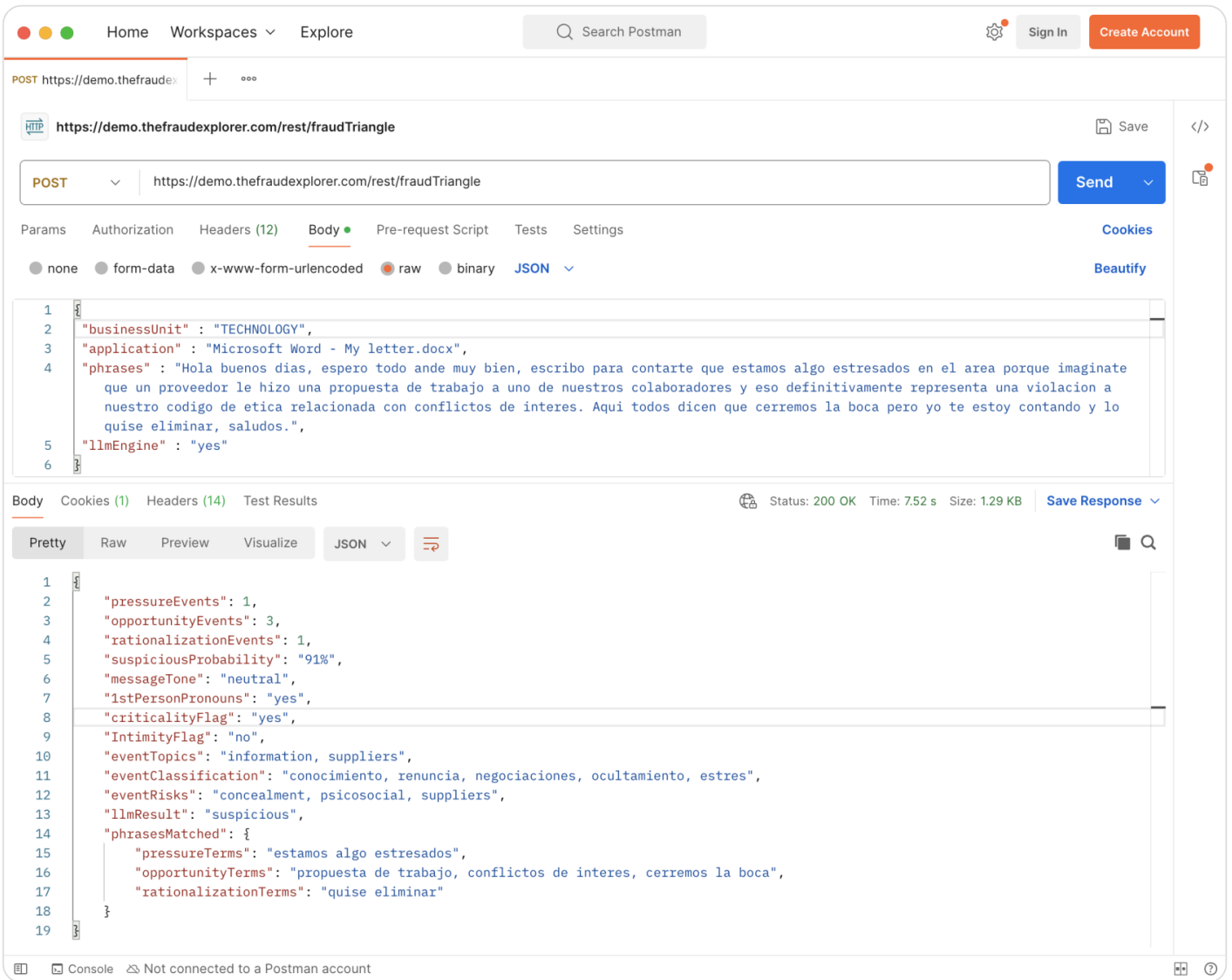
Insights del triángulo del fraude

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección <https://suinstancia/rest/fraudTriangle>, seleccione el método **POST** y luego en la pestaña **BODY** escriba:

```
{
  "businessUnit" : "TECHNOLOGY",
  "application" : "Microsoft Word - My letter.docx",
  "phrases" : "Hola buenos días, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos.",
  "IImEngine" : "yes"
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio entrega información de la cantidad de comportamientos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

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 #3

Created 23 July 2025 03:22:29 by Julian Rios

Updated 26 July 2025 02:16:26 by Julian Rios